

PHYSICAL SECURITY SYSTEMS

ASSESSMENT GUIDE

DECEMBER 2016

Office of Cyber and Security Assessments
Office of Enterprise Assessments
U.S. Department of Energy

PHYSICAL **S**ECURITY **S**YSTEMS **A**SSESSMENT **G**UIDE

December 2016

Table of Contents

Acronyms

AC	Alternating Current
ACD	Access Control Device
ANSI	American National Standards Institute
BMS	Balanced Magnetic Switch
CAS	Central Alarm Station
CCTV	Closed Circuit Television
CFR	Code of Federal Regulations
DOE	U.S. Department of Energy
EA	Office of Enterprise Assessments
ECS	Entry Control System
EOC	Emergency Operations Center
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive 12
IDS	Intrusion Detection System
ISSM	Integrated Safeguards and Security Management
LA	Limited Area
LLEA	Local Law Enforcement Agency
LSSO	Local Site Specific Only
MAA	Material Access Area
MC&A	Material Control and Accountability
ODSA	Officially Designated Security Authority
PA	Protected Area
PIDAS	Perimeter Intrusion Detection and Assessment System
PIN	Personal Identification Number
PPA	Property Protection Area
PSS	Physical Security Systems
PTZ	Pan-tilt-zoom
QA	Quality Assurance
RF	Radio Frequency
S&SP	Safeguards and Security Program
SAS	Secondary Alarm Station
SCIF	Sensitive Compartmented Information Facility
SNM	Special Nuclear Material
SPO	Security Police Officer
SRT	Special Response Team
SSSP	Site Safeguards and Security Plan
TID	Tamper-Indicating Device
UPS	Uninterruptible Power Supply
VA	Vulnerability Assessment
VMD	Video Motion Detector

Section 1: Introduction

Purpose

The Physical Security Systems (PSS) Assessment Guide provides assessment personnel with a detailed methodology that can be used to plan, conduct, and closeout an assessment of PSS. This methodology serves to promote consistency, ensure thoroughness, and enhance the quality of the assessment process.

The guide is intended to be useful for all assessors regardless of their experience. For the experienced assessor, information is organized to allow easy reference and to serve as a reminder when conducting assessment activities. For the new assessor, this guide can serve as a valuable training tool. With the assistance of an experienced assessor, the new assessor should be able to use the guide to collect and interpret data more efficiently and effectively.

Organization

This introductory section (Section 1) describes assessment methods and outlines their use. Sections 2 through 9 provide detailed guidance for assessing each major PSS subtopic:

- Section 2 – Intrusion Detection and Assessment
- Section 3 – Entry and Search Control
- Section 4 – Badging
- Section 5 – Barriers, Locks, and Keys
- Section 6 – Communications
- Section 7 – Testing and Maintenance
- Section 8 – Support Systems
- Section 9 – Systems Management.

Section 10 (Interfaces) contains guidelines to help assessors coordinate their activities within subtopics and with other topic teams. Information is provided on the integration process, which allows topic teams to align their efforts and benefit from the knowledge and experience of other topic teams. The section provides some common areas of interface for the PSS team and explains how the integration effort greatly contributes to the quality and validity of assessment results.

Section 11 (Analyzing Data and Interpreting Results) contains guidelines on how to organize and analyze data collected during assessment activities. These guidelines include possible impacts of specific information on other topics or subtopics, and some experience-based information on the interpretation of potential deficiencies.

Appendix A (Intrusion Detection System Performance Tests) provides procedures for testing the various systems and items of equipment that are commonly used in U.S. Department of Energy (DOE) facilities, with guidelines for evaluating test results. This appendix includes performance tests that are useful for evaluating a variety of intrusion detection systems (IDSs), such as:

- Exterior Perimeter Sensors
- Interior Sensors
- Perimeter Closed Circuit Television (CCTV)
- Interior CCTV
- Alarm Processing and Display.

Appendix B (Access Control System Performance Tests) contains effectiveness tests on entry control and detection equipment.

Appendix C (Communications Equipment Performance Tests) contains performance tests on radio equipment and duress alarms.

Appendix D (Support System Performance Tests) addresses the testing of equipment associated with power sources and tamper protection.

Appendix E (Personnel and Procedure Performance Tests) provides guidelines for designing and conducting site-specific tests of personnel and procedures. Candidate procedures and sample test scenarios are included.

General Considerations

While this guide covers a broad spectrum of assessment activities, it cannot address all security systems and variations used at DOE facilities. The methods that are described may have to be modified or adapted to meet assessment-specific needs, and assessors may have to design new methods to collect information not specifically addressed in this guide. Information in this guide is intended to complement DOE orders by providing practical guidance for planning, collecting, and analyzing assessment data. Assessors should refer to this guide, as well as DOE orders and other guidance, during all stages of the assessment process.

Using the Topic-Specific Methods

Sections 2 through 9 provide topic-specific information intended to help assessors collect and analyze assessment data. Each subtopic section is further divided into the following standard format:

- General Information
- Common Deficiencies/Potential Concerns
- Planning Activities
- Performance Tests (if applicable)
- Data Collection Activities.

Note that DOE Order 473.3A, *Protection Program Operations*, applies to the subtopics, in addition to other documents that may be relevant, such as:

- Executive Orders
- Site Safeguards and Security Plans (SSSPs)
- Implementation memoranda
- Memoranda of agreement
- Procedural guides.

These references are used as the basis for evaluating the assessed program and for assigning findings. It is useful to refer to the applicable references, particularly DOE guidance, during interviews and tours to ensure that all relevant information is covered.

General Information

The General Information section defines the scope of the subtopic. It includes background information, guidelines, and commonly used terms to help assessors focus on the unique features and problems associated

with the subtopic. It identifies the different approaches that a facility might use to accomplish an objective and provides typical examples.

Common Deficiencies/Potential Concerns

This section addresses common deficiencies and concerns associated with the subtopical area, along with a short discussion that provides additional detail. Information in this section is intended to help the assessor further refine assessment activities. Where appropriate, general guidelines are provided to indicate where a particular deficiency is likely to occur.

Planning Activities

This section identifies activities normally conducted during assessment planning. If applicable, specific activities or information available to assessors is identified for all planning phases. These planning activities include document reviews and interviews with the facility PSS managers. The detailed information in the Planning Activities section is intended to help ensure systematic data collection and to ensure that critical elements are not overlooked. Typically, the thoroughness of the planning effort directly affects the success of the assessment.

Performance Tests

General guidelines are provided to help the assessor identify site-specific factors that may indicate which specific performance tests may be particularly important. The details of PSS performance tests are provided in Appendices A through E.

Data Collection Activities

This section identifies activities that may be conducted to collect data. The information is intended to be reasonably comprehensive, although it cannot address every conceivable situation. Typically, these activities are organized by functional element or by the type of system used to provide protection. Activities include tours, interviews, observations, and performance tests. All activities are not usually performed for every assessment. The activities and performance tests to be accomplished are normally selected during the planning effort. The listed activities are those most often conducted.

Using the Tools in Each Assessment Phase

The assessment tools are intended to be useful during all phases of the assessment, including planning, conduct, and closure. The following summarizes the use of the assessment tools in each phase.

In the **planning phase**, assessors:

- Use the General Information section under each subtopic to characterize the program and focus the review.
- Perform the activities identified under Planning Activities to gather the information necessary to further characterize the program and focus the review.
- Review Common Deficiencies/Potential Concerns to determine whether any deficiencies are apparent, and to identify site-specific features that may indicate that more emphasis should be placed on selected activities.

- Assign specific tasks to individual assessors (or small teams of assessors) by selecting performance tests and specific items from the Data Collection Activities section. The assignments should be made to optimize efficiency and to ensure that all high-priority activities are accomplished.

- Review the guidelines under Section 10 (Interfaces) of this guide when assigning tasks to ensure that efforts are not duplicated.

- Prioritize and schedule data collection activities to optimize efficiency and to ensure that high-priority activities are conducted early in the process. A careful prioritization of these activities provides the opportunity to determine whether the available personnel resources and assessment time periods are sufficient to adequately evaluate the assessed topic.

- Review the applicable policy supplements to ensure that they are current with all applicable policy revisions, updates, and clarifications.

In the **conduct phase**, assessors:

- Use detailed information contained in the Data Collection Activities section to guide interviews and tours. Assessors may choose to make notes directly on photocopies of the applicable sections.

- Review common deficiencies, potential concerns, and previous findings after completing each data collection activity to determine whether any of the identified deficiencies are apparent at the facility. If so, assessors should then determine whether subsequent activities should be reprioritized.

- Review Section 11 (Analyzing Data and Interpreting Results) after completing each data collection activity to aid in evaluation and analysis of the data and to determine whether additional data is needed to evaluate the program. If additional activities are needed, assessors should then determine whether subsequent activities should be reprioritized.

In the **closure phase**, assessors:

- Direct specific attention to weaknesses that were identified during previous assessment activities.

- Determine whether the facility is complying with all applicable requirements.

- Use Section 11 (Analyzing Data and Interpreting Results) to aid in evaluating the collected data and assessing the impacts of identified deficiencies. This process will aid assessors in determining the significance of weaknesses that were identified, if any, and in writing the assessment report.

Performance Testing

Appendices A through E provide a set of common performance tests that may be used directly or modified to address site-specific conditions or procedures. Since performance testing is one of the most important data collection activities used in evaluating PSS, the information gathered during testing activities is rather extensive.

Performance testing differs from other data collection activities in several important ways. First, performance testing is the most labor- and time-intensive of all the data collection activities. Second, performance testing places the greatest demands on the resources of the assessed site and requires the highest degree of coordination and planning. Third, performance testing causes a potential for generating safety or security problems, and these concerns must be mitigated prior to initiating testing activities. In some cases, data can be gathered using simpler

data collection tools, and extensive performance testing may not be needed. Performance tests should always be carefully planned and coordinated before testing personnel arrive on site to ensure the most efficient use of time and resources.

Performance tests conducted by the PSS topic team may involve various tools and/or aids, personnel, and procedures, or any combination of these. The tools and aids include items that are readily available from commercial sources. Those items may be utilized by an adversary to circumvent detection using common knowledge techniques as well as information that is readily available from public information sources, such as internet sites. The ideal performance test stresses the system under examination up to the established limits of the site-specific threat, simulates realistic conditions, and provides conclusive evidence about the effectiveness of the security system.

Security system performance testing is intended to determine whether security equipment is functional, has adequate sensitivity, and meets its design and performance objectives under a variety of operating conditions. For example, tests for interior volumetric IDSs may incorporate walk tests, voltage variation, temperature and humidity variation, electromagnetic susceptibility, standby power tests, physical vibration, and handling shock tests.

Personnel performance tests are intended to determine whether procedures are effective, personnel know and follow procedures, and personnel and equipment interact effectively.

Performance tests must always be coordinated with appropriate facility personnel. Some of the tests require that personnel being tested remain unaware of the test. Particular care must be exercised to ensure that these tests are well coordinated and safety factors carefully considered.

Unfortunately, realistic conditions are frequently difficult to simulate because of safety concerns, time and resource constraints, and the heightened security posture that often results when site personnel are aware that an assessment is under way.

The process of identifying specific systems to test is generally based on information that is identified during document reviews, interviews, and various onsite data collection activities. If this information leads the assessors to question whether any weaknesses may be associated with a specific protection program or a particular adversary path, or if the maintenance history of a system indicates a potential concern, the associated systems should be evaluated by testing. It is important to not concentrate on one aspect or component of a system at the expense of others when tests are conducted, although it may not be necessary to test all components to determine overall effectiveness. For example, when several doors are installed in a barrier wall and they are all equipped with identical alarm equipment, testing a sample of the doors may be sufficient to determine the overall effectiveness of the alarm equipment on the doors.

Validation

Validation is the process used to verify, with site representatives or points of contact, the accuracy of the information that assessors obtain during data collection. The site representatives or points of contact should understand the specific point that is being validated, along with its potential impact on overall PSS performance. During this process, site personnel should have the opportunity to provide other relevant information that may mitigate apparent weaknesses. These procedures, discussed in the DOE Office of Enterprise Assessments (EA) Appraisal Process Protocols, include on-the-spot validations, daily validations, and summary validations. On-the-spot validations verify the data at the time of collection. These validations are particularly important during performance testing because a number of people may be present and it is frequently difficult to reassemble these same people for the daily and summary validations. All on-the-spot validations should be re-verified during daily validations, which are normally conducted at the end of the day during the data collection phase of the assessment. The summary validation

is usually conducted at the end of the data collection phase of the assessment. Team members must keep track of the information covered in on-the-spot and daily validations so that it can be reiterated during the summary validation.

Characterization of the Physical Security Systems Topic

Physical security is defined as the use of intrusion detection and assessment, entry and search control, barriers and locks, communications, testing and maintenance, and support systems and interfaces to deter, detect, annunciate, assess, delay, and communicate an unauthorized activity. An effective PSS program employs a complementary combination of these components (see Figure 1), augmented by practices and procedures specific to each location.

All DOE security assets, both tangible and intangible, are protected from theft, diversion, sabotage, espionage, and compromise that might adversely affect national security, program continuity, the environment, or the health and safety of employees or the public. There are four basic asset groups:

- Special nuclear material (SNM) and vital equipment
- Classified information
- Unclassified sensitive information
- Property and unclassified facilities.

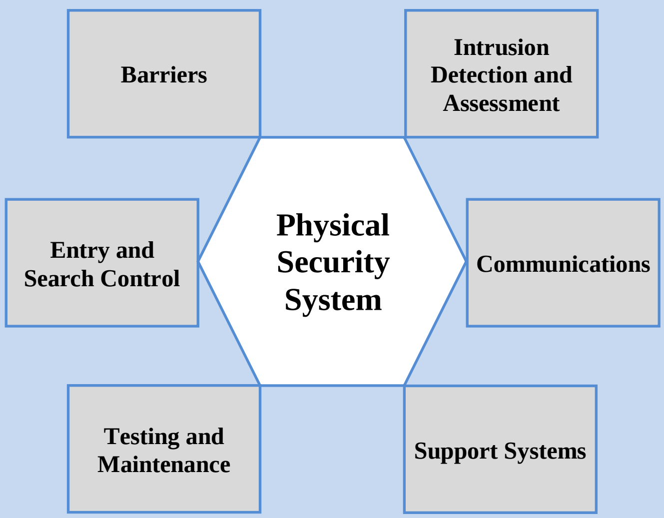


Figure 1. Physical Security Systems Components

SNM is defined and categorized according to quantity, composition, and attractiveness to adversaries. Each category of SNM requires specific protection measures during storage, transit, and use. Most of these measures are discussed in DOE Order 473.3A.

Vital equipment is defined as "equipment, systems, or components whose failure or destruction would cause unacceptable interruption to a national security program or an unacceptable impact on the health and safety of the public." Site offices are responsible for identifying the vital equipment located at facilities under their purview.

The level of protection afforded classified matter depends upon the level of classification or category assigned: Top Secret, Secret, or Confidential. Classified matter can be information, documents, parts, components, or other material.

Increased levels of protection are provided to high-consequence assets. The most significant protection efforts center on nuclear weapons and Category I SNM. Also, IDSs and entry control systems (ECSs) that protect classified communications centers and computer centers are of concern to the PSS topic.

Protection standards are specific to the type of security interest, as well as to specific targets. Consequently, various levels of analytical and design sophistication are applied to protect different assets. The design of a system requires an engineering perspective, incorporating site-specific requirements determined by vulnerability assessments (VAs) and resulting in a level of protection consistent with DOE guidance. Levels of protection for particular safeguards and security interests are provided in a graded fashion in accordance with the potential risks.

PSS provide protection along adversary penetration paths where force, deceit, or stealth tactics may be employed to defeat the system (see Figure 2, an example of layered protection of SNM). Force, deceit, and stealth are characterized as:

- **Force:** Adversary actions directed at overcoming elements of the physical security system by overt aggressive activities, which the adversary expects to be detected. The adversary is therefore prepared to forcefully respond to site interdiction.

- **Deceit:** Adversary actions directed at overcoming elements of the PSS by normal submission to an element with the expectation that unauthorized conditions, such as a fake badge or shielded material, will not be detected.

- **Stealth:** Adversary actions directed at overcoming elements of the physical protection system by avoiding or deactivating these elements in an attempt to prevent detection.

One approach in determining whether assets are at risk is to identify the existing adversary paths leading into and out of the target area. This is perhaps best visualized by color-coding a large site map and highlighting the layers of protection afforded the security assets. This process identifies the various components of the PSS (i.e., barrier systems, ECSs, and interior and exterior intrusion detection and assessment systems). A color-coded map helps the assessors visualize the overall methodology used by the site and allows evaluation of system weaknesses. Also, this will aid in the selection of performance tests. The completed site map, marked to indicate the various layers of protection comprising the PSS, should be compared with a verified listing of assets to ensure that all assets are afforded appropriate protection. The assessor can then begin to identify and describe the component parts of the PSS.

Data Collection Guidelines

This section provides general data collection guidelines for briefings, document reviews, limited-scope performance tests, facility tours, and interviews. More specific guidance is included in the individual subtopic sections.

Data collection begins as soon as a site is selected, and it continues throughout the planning and conduct phases of the assessment. An integral part of the assessment planning process involves collection, review, and analysis of data relative to the site. Knowledge of the site-specific assets and the protection methods used provides insight into the site’s mission, operations, and processes.

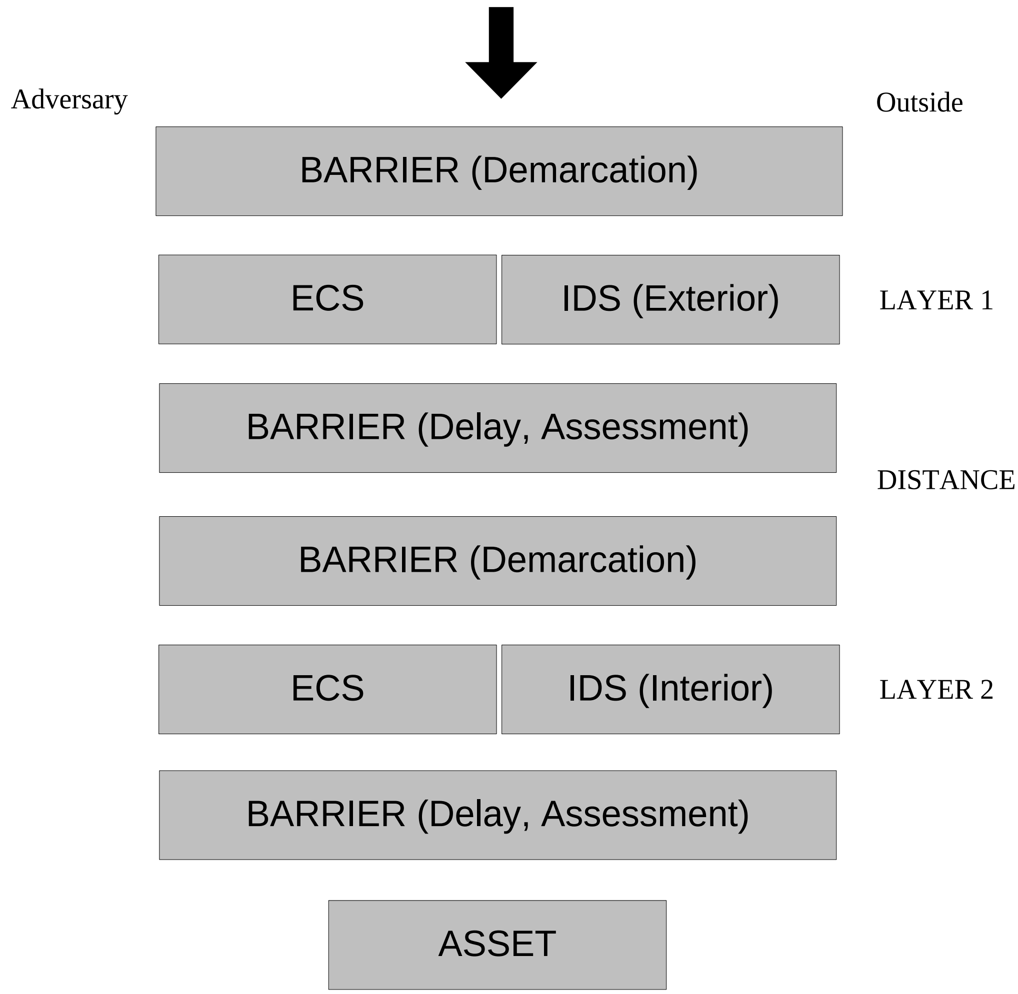


Figure 2. Schematic Adversary Path to an SNM Asset

Briefings

During the **planning phase**, briefings are presented by the site office and contractor representative to provide the PSS assessment team with a broad understanding of the site mission. This information is supplemented by a review of documents and interviews with site representatives.

The **conduct phase** begins with an onsite meeting between the assessment team and the DOE site office point of contact to:

- Review follow-up items from planning activities.
- Work out details of the assessment schedule (for example, specific points of contact for each activity).
- Discuss any issues that may have developed subsequent to planning activities.

Document Reviews

To focus the assessment process and ensure that assessment resources are applied appropriately, during the planning phase the PSS assessment team compiles a listing of site assets described in the SSSP, grouping

them into appropriate categories. As the assessment progresses, assets should be confirmed with topic teams dealing with material control and accountability (MC&A) and classified matter protection and control. Assessors can draw certain conclusions and inferences based on the consequence of loss of these assets and, in so doing, can further focus assessment efforts.

Document reviews are an important part of the evaluation of PSS effectiveness. Document reviews begin during the planning phase with the review of the SSSP, survey and assessment reports, and other documents. These documents reveal the physical protection philosophy and approach taken to implement the safeguards and security requirements mandated by DOE orders.

Information obtained from document reviews establishes the assessment baseline for:

- Verifying information received from briefings, tours, and interviews
- Determining the site-specific threat
- Identifying site/facility assets
- Evaluating PSS corrective actions
- Establishing the response posture and protection strategy
- Understanding standard operating procedures.

Basic documents to be reviewed include:

- Organization charts
- SSSP
- Site security plans
- Security plans for temporary material access areas (MAAs)
- Decontamination and decommissioning plans
- Listing of waivers and exceptions
- Past survey reports and EA assessment reports
- Facility asset list
- Maps/drawings showing security areas, buildings, security posts, vital equipment areas, and SNM storage areas.

VAs are also reviewed to clarify the facility's evaluation of all potential threats to their security assets, whether from external forces or internal personnel. The review should evaluate pathways that might be used in these scenarios and characterize pathways in terms of detection and delay accumulated by the adversary. The overall delay for each pathway is calculated and compared to protective force response times to determine the probability that the protective force will interrupt the adversaries before they can access the target. By reviewing these assessments, assessors can better identify the systems that the facility considers to be most essential to asset protection. The following are some considerations for review of VAs:

- Priority of site-specific threats

- Identification of "worst-case" (lowest probability of detection and/or shortest amount of delay) pathways into a facility

- Identification of systems (detection, assessment, delay) that are most critical in providing protection for DOE assets

- Determination of the assumed detection probabilities for each system

- Determination of the credit taken by the facility for assessment (immediate assessment vs. delayed assessment)

- Identification of the last possible point at which an adversary must be detected to allow adequate response/adversary interruption by the facility protective force

- Graded protection and defense-in-depth

- Comparison of vulnerabilities against findings and resolution of past EA assessments and operations office surveys.

Records and procedures are also reviewed. **Records** include operations logs; test records; PSS maintenance, testing, and repair records; trend analysis information; occurrence reports; force-on-force after-action reports; and other records identified during the course of the assessment. **Procedures** include protective force post orders, maintenance procedures, MC&A procedures, and facility operating procedures. The assessment team reviews these items to determine whether:

- Required PSS records are kept.
- System tests are performed and documented as required.
- System maintenance is performed as required.
- PSS procedures are comprehensive and effective.
- Anomaly resolution is timely and effective.
- The overall protection afforded DOE assets has been considered.

Limited-Scope Performance Tests

Limited-scope performance tests are selected based largely on the analysis performed during the planning phase of the assessment and on information derived from facility tours and interviews with operations office and contractor representatives. Typical test measures verify whether:

- PSS are accurately characterized in VAs and security plans.
- Response times are consistent with those identified in security plans.
- Equipment is tested and calibrated according to traceable specifications.
- Procedures are complete and describe the actual methods of operation.
- Personnel adhere to procedures in performing their activities.
- Personnel are knowledgeable of their duties and responsibilities.
- Equipment is in good repair.

Facility Tours

The assessment team generally tours the facility as early as possible. More detailed tours of key areas are scheduled as needed.

Although assessors are likely to examine facility drawings and analyze potential adversary paths, facility tours are essential to gain the level of understanding that the assessment team requires. The purposes of these tours are to:

- Become familiar with the site and facility layout.

- Observe the actual layout of the overall PSS and individual elements of the system.

- Verify that the documentation previously examined accurately reflects the current conditions and configurations at the site.

- Ensure that the systems described in documentation are implemented and operational.

- Identify anomalies or deficiencies that require further investigation.

- Select specific areas or components as candidates for performance testing.

Tours provide the opportunity to place the PSS documentation and briefings into perspective, because the assessors can witness the operating environment and note the intangibles that affect system design and operation. To obtain maximum benefit from the tour, the topic team should:

- Minimize unnecessary inconvenience to tour guides and facility operations and personnel.

- Try to observe procedures during normal operations (e.g., observe vehicle search procedures while testing equipment at a post).

- Have the people who normally work in the area demonstrate the procedures rather than having a supervisor demonstrate how they think the procedure is performed.

- Take notes on areas that may require further review (e.g., vault thickness, protection against penetrations into vaults).

- Ensure that tour logistics are carefully arranged.

During the initial tours, assessors should verify:

- Locations and boundaries of MAAs and Protected Areas (PAs)
- Category designation of MAAs and PAs
- Locations of MAA and PA access portals
- Locations of normal transfer points and paths between MAAs
- Locations and types of security equipment installed
- Location of the alarm stations.

Additionally, assessors should confirm:

- General quality and condition of the physical barriers

- Entry control procedures and methods employed at access portals (contraband detection equipment and procedures, badge checks, badge exchanges, card readers, biometrics)

- Type of storage areas (vaults, vault-type rooms, alarmed rooms, safes, locked filing cabinets, locked rooms)

- Location of emergency exits

- Types and approximate quantities of SNM in use or being processed.

Interviews

Interviews clarify impressions and allow insight into facility operating procedures. Interviews with personnel at all organizational levels are recommended. Frequently, discussions with personnel involved in "hands-on" operations reveal whether management's policies and directives are effectively communicated and implemented, and whether the systems actually function as described in the documentation.

Personnel to consider interviewing include DOE and contractor security managers, facility managers and staff, vault/vault-type room custodians, security police officers (SPOs), security technicians/specialists, PSS maintenance personnel, systems engineers and programmers, and central alarm station (CAS) and secondary alarm station (SAS) operators. Other personnel may be interviewed as needed. Interviews are not necessarily formal, and often take the form of discussions during facility tours or performance testing.

Safeguards and Security Program

The Department is committed to conducting work efficiently and securely. DOE Policy 470.1A, *Safeguards and Security Program* (S&SP), provides a framework that encompasses all levels of activities and documentation. The framework includes seven components to facilitate the orderly development and implementation of S&SP guiding principles and core functions.

The guiding principles of S&SP are:

- Safeguards and security considerations are thoroughly integrated with all aspects of mission accomplishment.
- Protection requirements are commensurate with the consequences of loss or misuse of the protected asset.
- Responsibility for the implementation of protection measures resides with DOE line management elements responsible for mission accomplishment.
- Authority is delegated to appropriate levels to promote efficiency and effectiveness.
- Program oversight ensures that opportunities for improvement, both in effectiveness or efficiency, are identified and acted upon.
- Managers are empowered to make risk management decisions as necessary to support mission accomplishment.
- Program focus is upon overall mission performance.

The core functions of S&SP are:

- Identify all protection needs for the Department.
- Establish clear roles and responsibilities for safeguards and security.
- Implement Departmental policy through line management.
- Establish safeguards and security oversight programs to ensure that policy implementation meets established standards.
- Seek and implement continuous improvements and efficiencies.

For the purposes of this assessment guide, EA has established four general categories that encompass the concepts embodied in the guiding principles and core functions of S&SP:

Line Management Responsibility for Safeguards and Security. This category encompasses the corresponding S&SP guiding principles that relate to management responsibilities (i.e., line management responsibility for protection of DOE assets, clear roles and responsibilities, and balanced priorities).

Personnel Competence and Training. This category encompasses the S&SP guiding principle related to competence of personnel (i.e., competence commensurate with responsibilities). It also includes DOE requirements related to ensuring that personnel performing safeguards and security duties are properly trained and qualified, and incorporates the need for sufficient training and certification along with an appropriate skill mix.

Comprehensive Requirements. This category encompasses the corresponding S&SP guiding principles and core functions that relate to policies, requirements, and implementation of requirements (i.e., identifying safeguards and security standards and requirements, tailoring protection measures to security interests and programmatic activities, providing operations authorization, defining work, analyzing vulnerabilities, identifying and implementing controls, and performing work within controls).

Feedback and Improvement. This category encompasses the corresponding S&SP core function (i.e., feedback and improvement) and DOE requirements related to DOE/National Nuclear Security Administration line management oversight and contractor self-assessments.

The categories above are used only to organize information in a way that will help assessors gather data about management performance in a structured and consistent manner. EA has identified general categories of information that would be expected in an integrated safeguards and security management (ISSM) program.

Section 2: Intrusion Detection and Assessment

General Information

DOE orders stipulate that IDSs and/or visual observation by protective force personnel be utilized to detect unauthorized entry and/or presence in security areas that require protection. Typically, the procedures to meet these requirements are documented in approved site security plans.

The following IDS elements are covered in this section:

- Alarm annunciation, monitoring, and control systems
- Exterior and interior sensors
- Power supply
- Assessment and response
- Lighting.

The testing and maintenance program is addressed in Section 7.

In addition to patrols and visual surveillance provided by the protective force, the alarm detection and assessment systems are fundamental PSS components. To be effective, audible alarms must be discernable. Alarm displays must be clearly visible and must identify the location and type of alarm, and the operator interface must allow for alarm recognition by the operator. Alarm communication lines and other detection devices require continuous supervision to preclude any covert attempt to bypass the alarm system, and to ensure an appropriate and timely response. To achieve an acceptable degree of assurance that the PSS works properly, facility management must provide for adequate equipment, an effective testing and maintenance program, and a sufficient number of trained personnel to operate the alarm and assessment equipment.

IDSs consist of both an alarm and an assessment system and are usually layered for both interior and exterior applications. Exterior systems are designed to provide the earliest possible detection of an unauthorized intrusion, as far away from the security interests as possible. The interior IDS may be even further divided into layers according to the configuration of security areas and the required levels of protection.

At SNM facilities, the outermost layer of the exterior systems is usually the perimeter intrusion detection and assessment system (PIDAS), which typically consists of multiple and complementary electronic sensors, such as:

- Microwaves
- Active and passive infrared sensors
- Capacitance sensors
- Fence disturbance systems
- Buried coaxial cable sensors
- Seismic and pressure sensors
- Taut wire.

Exterior systems must be capable of withstanding the environmental conditions in which they are deployed. Properly designed systems generally use two or more types of complementary sensors, depending on the operating environment and design parameters. Typically, the PIDAS also includes fixed-position CCTV coverage for timely assessment of alarms generated in the PIDAS bed. PIDAS alarms normally annunciate in the CAS and SAS, where the alarm console operators can acknowledge the alarm, assess its cause, and direct a response as necessary.

Although design characteristics differ depending on the systems in use, the exterior sensors are intended to ensure that a person above a specific weight crossing the perimeter at certain speeds will be detected whether walking, running, jumping, crawling, rolling, or climbing in the sensor's detection zone. Sensor systems are required to have adequate coverage in all weather and light conditions, overlap to eliminate dead areas, and be tall enough to deter bridging. Also, it is essential that detection zones contain no dips, high ground, or obstructions that could provide a pathway for an individual to avoid detection.

CCTV systems used in conjunction with alarm and detection systems are most effective when they can automatically call the operator's attention to an alarm-associated camera display, and the camera's picture quality, field of view, and image size is such that the operator can easily recognize human presence. Tamper protection and loss-of-video alarm annunciation are essential characteristics of the system if the cameras serve as the primary means of alarm assessment. Video recorders, when used with the CCTV system and when initiated by alarm signals, are most useful when they operate automatically and are rapid enough to accurately record an intrusion. Video capture systems, if used, provide pre-alarm, alarm, and post-alarm video images of the alarmed zone.

Interior systems are designed, installed, and maintained in a manner to eliminate gaps in detection coverage and to prohibit adversaries from circumventing the detection system. Interior IDSs typically consist of one or more of the following technologies:

- Passive infrared
- Microwave
- Video motion detection
- Balanced magnetic switch (BMS)
- Disturbance detection.

These IDSs are normally designed to protect specific security areas, such as:

- PAs
- Limited Areas (LAs)
- MAAs
- Vaults
- Vault-type rooms
- Igloos/bunkers
- Security areas.

These systems employ various technologies that detect:

- Physical movement
- Heat
- Cable tension
- Vibration
- Pressure
- Capacitance.

IDS sensors are used to detect movement within a specific area. Sensor coverage must ensure that IDS coverage surrounds the security interest in order to detect attempted physical access via any credible pathway.

A BMS or other equally effective device must be used on each door or movable opening to detect attempted or actual unauthorized access. Each BMS must initiate an alarm when an attempt is made to defeat the switch by substituting an external magnetic field, as well as when the leading edge of the associated door is moved 1 inch (2.5 centimeters) or more from the door jamb.

Assessment measures range from the use of auto-focus CCTV cameras systems to the deployment of protective force personnel to visually observe the area where the alarm occurred.

The field device network is the array of sensors and data transmission equipment that communicates to the primary and secondary host computers. Communication between host computers and field devices of the system should be redundant and independently routed, as required by DOE policy. Field devices consist of local processors, input/output panels, and multiplexing units, depending on the manufacturer's system configuration. The field device network should provide randomly polled digital supervision that detects and annunciates communications interruptions or compromised communications between any field device and the host computers.

Since alarms and detection systems require a power source for operation, an auxiliary power source consisting of an uninterruptible power supply (UPS) and generator must be available, and switchover must be immediate and automatic if the primary power source fails. In most cases, immediate and automatic switchover does not occur if a generator is the only source of backup power; the UPS is needed to handle the immediate switchover, and the generator assumes the role once it reaches full power.

To ensure effective operation of alarms and detection devices, managers must provide for a regular test and maintenance program that includes the periodic testing of equipment and circuits and the thorough assessment of equipment and circuits by qualified service personnel. Also, records of these tests are required to include the date of the test, the name of the person conducting the test, and the results. Details on assessing the testing and maintenance program are discussed in Section 7.

Frequently, IDSs and ECSs are separate systems, interfaced to provide information to the system operator. In many systems, normal access control and other work-related activities are processed without operator interaction. Records of such transactions are recorded for historical purposes.

The main purpose of an IDS is to alert the protective force to an intrusion, aid in assessment of the cause of the alarm, allow the protective force to track intruder progress toward a target, and aid in assessing intruder activity and characteristics (for example, the number of intruders and whether they are armed). Protection systems normally include a suitable means of assessing alarms and provide for an appropriate response. The protective force is usually responsible for monitoring the IDS and responding to IDS alarms.

Security lighting is of primary importance in the operation of an effective alarm and detection system. Effective lighting may provide a deterrent to adversary intrusion, and also assists the protective force in locating and assessing alarm initiations and provides for effective use of CCTV as a surveillance and assessment tool. Lights must have a minimum specified luminescence at ground level for specific areas, a regular power source, and an emergency backup lighting capability. Lights should not cause glare or bright spots in CCTV camera images, especially if CCTV is the primary means of assessment.

Common Deficiencies/Potential Concerns

False and Nuisance Alarms

One of the most common problems with IDSs is that they may generate an inordinate number of nuisance alarms. Many systems are susceptible to false and nuisance alarms induced by high winds, animals, heavy snow, lightning, vehicular vibration, and wind-blown dust and debris. These systems include:

- Microwave sensors
- Infrared sensors
- Electric field sensors
- Seismic sensors
- Buried sensors.

Improper installation (improper tension or insulation coupling) can also cause unacceptable false alarm rates in electric field sensors. Seismic sensors may produce nuisance alarms if installed near fences, power poles, guy wires, or roads where vehicles generate heavy ground vibration. Video motion detectors (VMDs) are susceptible to nuisance alarms induced by reflected light, cloud motion, vehicle headlights, and camera vibration due to wind. A high rate of false and/or nuisance alarms may lead the protective force to ignore or improperly assess an intrusion.

Improper Installation, Calibration, or Alignment

Improper installation, calibration, or alignment of sensors may significantly reduce sensitivity, contribute to false alarms, and allow an unauthorized intrusion. For example, insufficient offset may allow intruders to crawl under or jump over a bistatic microwave beam at the crossover point (the point where adjacent zones overlap). Also, VMDs require extensive maintenance and calibration for proper operation, and audio detectors must be calibrated carefully to avoid nuisance alarms caused by common background noises. Effective operation of a CCTV system is frequently diminished when the system is incorrectly installed or aligned. If the camera is improperly placed or aligned, there may be "holes" in the coverage that permit an intruder to cross the isolation zone unobserved. Additionally, if the field of view of the camera is too long for the camera lens, an intruder at the extreme end of the field of view may not be adequately observed.

Tamper Protection for BMS, IDS Enclosures, Junction Boxes, and Power Sources

Permanent junction boxes, field distribution boxes, cable terminal boxes, and cabinets (equipment that terminates, splices, and groups interior or exterior IDS input or that could allow tampering, spoofing, bypassing, or other system sabotage) must be afforded tamper protection. Tamper protection and appropriately-mounted hardware reduce the chance of bypass or defeat of the sensors and sensor components. The primary and backup power sources for IDSs are susceptible to tampering. Power switches, inverters, and generators should be protected but are often overlooked during protection planning and installation. Exterior fuel tanks and filler points are especially vulnerable. For example, an inoperable filler point or contaminated fuel tank may nullify all backup power sources. If the primary power source fails, the protection systems become inoperable and DOE assets become vulnerable.

Inadequate Testing and Maintenance Program

Most PSS failures are the direct cause of an inadequate testing and maintenance program. Like an automobile, the lack of maintenance and operation (testing) usually results in equipment failure. For this reason, the testing and maintenance program is one of the most important features of any protection system. An effective program normally includes provisions that require facility technicians, augmented by service representatives, to perform all tests, maintenance, calibrations, and repairs necessary to keep the detection and assessment systems operational. An inadequate program that results in frequent system failure, cursory testing procedures, or an inordinate number of items of equipment awaiting repair may indicate a lack of management attention. Details of assessing the testing and maintenance program are discussed in Section 7.

Failure to Properly Assess and Respond

A number of factors may affect assessment and response. For example, a high rate of nuisance and false alarms may degrade operator response to genuine alarm conditions. Failure of a system to adequately identify alarm type and specific location may also degrade response. The latter is usually most evident when systems do not clearly differentiate between tamper-indication, line-supervision, and intrusion alarms, or when multiple sensors are monitored by a single alarm point. For computer-based systems, problems may arise because of erroneous software modifications and system configurations that cause program errors. It is important that the signal received from the detection device provide identifiable evidence of the actual occurrence so operators can properly assess the situation and respond accordingly.

Planning Activities

During assessment planning activities, assessors review available documents and interview points of contact. Elements to cover include:

- Review of the site mission (obtained from a review of the documents and from interviews with site office personnel and site representatives)

- Review of:

  - Organization charts
  - SSSP
  - Site security plans and procedures
  - Security plans for temporary MAAs
  - Decontamination and decommissioning plans
  - Deviations, both approved and requested
  - Past site office survey reports and EA assessment reports
  - Self-assessment reports
  - Site/facility asset list
  - Alarm procedures
  - Site maps/drawings indicating:

    - Security areas (property protection areas [PPAs], LAs, PAs, security areas, MAAs, vaults, vault-type rooms)
    - Critical facilities
    - Controlled areas
    - Building definitions
    - Locations of security posts
    - Classified matter areas
    - Vital equipment areas
    - SNM storage areas
    - Transfer routes
    - Lighting diagrams

- Review of lists showing:

  - Types of sensors employed
  - Local alarm reporting devices
  - Data transmission systems
  - Console equipment descriptions

- Review of the assessment methodology employed (CCTV, video, and/or patrol response)
- Review of the VA, including consideration of:
  - Application of the design basis threat
  - Whether the threats identified by the site address local characteristics, including the insider threat
  - Priority of site-specific threats
  - Target definition and locations
  - Graded and defense-in-depth PSS
  - Pathways providing lowest detection and/or shortest delay
  - Presentation of the VA results in the SSSP
  - Listing of the protective elements identified in the VA for each security interest (review the VA results in the SSSP to determine whether the key VA results are in the SSSP and whether any assumptions in the VA should be validated during the assessment)
  - Comparison of vulnerabilities against findings and resolution of past EA assessments and site office surveys
- Review of protective methods employed at the location to be assessed
- Determination of the type and location of potential targets (to further focus assessment efforts, compile a list of site assets, group them into appropriate categories, and determine potential impacts related to their loss).

Performance Tests

The following performance tests are recommended for alarms and intrusion detection devices:

- Exterior Perimeter Sensors (Appendix A, Part 1)
- Interior Sensors (Appendix A, Part 2)
- Perimeter CCTV (Appendix A, Part 3)
- Interior CCTV (Appendix A, Part 4)
- Alarm Processing and Display (Appendix A, Part 5).

Data Collection Activities

Alarm Annunciation, Monitoring, and Control Systems

A. Assessors should review alarm records to determine false/nuisance alarm rates. This may involve reviewing alarm logs for a specified period (for example, two weeks) and determining the number of alarms during that period. Alternatively, the assessor could review the facility's plots of alarm rates, if such plots are maintained. Any abnormally high alarm rates should be identified and the causes discussed with the facility representatives (including measures taken to eliminate false/nuisance alarm sources). The accuracy of alarm records can be investigated by comparing alarm plots against alarm logs or alarm plots/logs against computer records for a

specified period. When reviewing alarm records, the assessor should clearly understand the facility's definitions of false alarms and nuisance alarms and how they are assessed. The assessor should also consider interviewing alarm system operators to determine their understanding of false/nuisance alarm rates and make sure that they are consistent with facility definitions. Operators' ability to consistently make judgments as to whether alarms are considered false or nuisance will greatly affect false and nuisance alarm rate calculations.

Exterior and Interior Sensors

B. During the PIDAS review, assessors should examine the various types of sensors to determine whether they are complementary (that is, whether they consist of different sensor types that cannot be defeated by the same means, not just multiple layers of the same sensor). Assessors should also confirm the existence of an effective testing and maintenance program for the PIDAS. Assessors should check the condition of the PIDAS bed for obstructions, mounds and valleys, and other terrain features that an adversary could use to avoid the detectors. Crossover and interface points should also be checked to determine whether voids or blind spots occur in sensor coverage. Particular attention should be given to the identification of PIDAS sectors susceptible to bridging as a result of their close proximity to tall buildings, fences, telephone poles, light and camera structures, or overhead lines capable of supporting the weight of an intruder. Similarly, tunnels that pass beneath PIDAS sectors should be reviewed to determine whether they are adequately protected.

C. Assessors should tour the CAS and SAS, visually assess equipment, interview operators, and verify information gathered previously during document reviews. Items to be checked include operability of equipment, operators' familiarity with equipment, and measures to protect equipment from tampering. System operators must recognize and acknowledge alarms reported from the field and respond appropriately. Interviews with system operators will reveal how well they understand their responsibilities.

D. At each exterior security area where a PIDAS is used, assessors should determine:

- The number and configuration of sensors
- Sensor alarm logic (e.g., 1 of 2, 2 of 3)
- Test frequency and methods
- Preventive maintenance frequency and methods
- Tamper-indicating provisions
- Provisions for repairing component failures.

E. Assessors should review documents and interview security staff to determine the method used to detect intrusion at each security area. If more than one method of detection is used at a security area (for example, an electronic alarm system and direct observation from guard towers), assessors should determine:

- How the systems complement each other
- Which is considered the primary means of detection
- Whether the combination (primary and backup) is effective.

F. At selected interior security areas (for example, MAA buildings) and storage areas, assessors should determine:

- The types of sensors used to protect building perimeters (including doors, windows, and other penetrations)
- Testing and preventive maintenance frequency and methods
- Tamper-indicating provisions
- Conditions for placing a zone portal in access
- Provisions for repairing component failures.

G. Assessors should determine whether the facility has more than one central electronic alarm system and, if so, the area that each system covers. A facility with two well-defined geographical areas may have a separate alarm system for each. For each separate electronic alarm system, assessors should determine:

- Whether there are multiple SASs
- Central processing unit switching capability
- Tamper alarm features
- Adequate primary and backup power supply.

This information can be gathered by document reviews or interviews with security staff. However, assessors may need to interview the responsible system engineers to accurately determine the technical aspects of the system. Conducting such interviews in the CAS/SAS may allow a better understanding of the system and its interfaces.

H. Assessors should verify that the SSSP identifies means for providing intrusion detection capability when primary systems are out of service. Implementation of the measures can also be verified, generally by reviewing the CAS or protective force supervisor logs or maintenance records to determine when equipment was out of service and to verify that compensatory measures were implemented during those periods.

Power Supplies

I. Auxiliary power supplies are required for all security systems. Assessors should validate the operability of these supplies. Power supplies are normally tested concurrently with the PIDAS lighting test.

Assessment and Response

J. Assessors should verify complete coverage of the security area perimeter. This activity is particularly applicable at areas with alarmed fence lines that delineate a security area perimeter and that rely on protective force visual observation posts to assess alarms. An effective method of verifying complete coverage is to have two testers walk along both fence lines (isolation zone) while assessors are stationed in the CAS assigned responsibility for assessment of that portion of the perimeter. Each portion of the perimeter can be checked sequentially. In this manner, the assessors can verify that no blind spots occur along the perimeter that might permit an adversary to breach the boundary without being detected and assessed. This activity can be facilitated with two or more assessors who rotate from post to post. The overlap points between zones can also be checked more readily with two or more assessors in adjacent observation posts.

K. Assessors should observe CCTV display monitors during a range of conditions, such as at different times of the day and night and under various weather conditions if possible. Alternatively, the assessor may request facilities that have a video recording capability to provide tapes recorded during different weather conditions, if available. Assessors should review the monitors or recordings to determine whether the CCTV systems provide appropriate data under varying light and weather conditions. Assessors should also verify that camera and recorded video call-ups are rapid enough to capture adversary activity. This is often done as part of the PIDAS assessment, and it is performed once during the day and again at night.

L. Assessors should interview security staff and review documents to determine the areas where direct visual observation is the primary means of detecting intrusion or assessing alarms. Assessors should determine the type of post (for example, tower, portal, continuous patrol), assessment aids available to protective force personnel (for example, search lights, night vision devices, binoculars), and the methods used by the facility to test effectiveness and maintain the SPO's level of vigilance. Assessors should determine:

- The operability of equipment
- Power supplies
- Measures to protect equipment from tampering
- Fields of view
- Adequacy of lighting
- Blind spots or obstructions
- Overlap with adjacent zones.

Lighting

M. Assessors should interview security staff, review documents, and conduct performance tests to determine:

- Effectiveness of lighting levels at:
  - Portals
  - Security area perimeters
  - Exterior and interior areas that rely on CCTV for assessment
- Adequacy of normal and auxiliary lighting system power supplies
- Procedures that are implemented if lighting fails
- Methods for monitoring lighting systems
- Procedures for reporting and replacing burned-out lights and failed equipment.

N. Assessors should observe the lighting during nighttime tours of the facility while lights are on primary power and then on auxiliary power. The lighting levels should be observed from a variety of locations, including key visual assessment posts (for example, towers). The CCTV monitors in the CAS/SAS and other selected posts (if any) should also be observed to determine the adequacy of lighting. One method of determining the adequacy of lighting is to have one or more persons (dressed in various contrastable color clothing) stand in various areas, as directed by the assessors who are stationed in visual observation posts or monitoring CCTV cameras in the CAS/SAS. The assessors should direct the individual to stand in locations where light levels are low or contrast ratios are high. The assessors should determine whether there are blind spots and whether the lighting is adequate to distinguish between humans and animals at any location in the observation zone. If feasible, the lighting should be observed during a variety of conditions (for example, clear weather and rain or fog). Items to check include:

- Lighting levels
- Light/dark contrast
- Glare/reflection
- Shadows
- Inoperative bulbs.

Light meters may be used to check lighting levels and contrast ratios in various areas.

O. Assessors should determine the vulnerability of lighting systems to sabotage by reviewing lighting circuit and power supply diagrams and touring areas critical to the lighting systems (for example, switchyards, transformers, circuit breaker panels, power lines, engine-generator sets, and UPS). Assessors should determine:

- Whether all lights at a security area perimeter are on a single circuit (as opposed to having every other light on a second circuit)

- Whether the electric power supplies are vulnerable to single-point failures (for example, a circuit breaker)
- Whether there are provisions for controlling access to areas containing components critical to the lighting system
- Self-testing features
- Methods for modifying system hardware and software
- Whether there are provisions for maintaining assessment capability if the lighting fails.

Section 3: Entry and Search Control

General Information

Entry and search controls are established to prevent unauthorized access to security areas, theft of classified information, removal of SNM, sabotage of vital equipment, and introduction of contraband. These controls may include access identification systems, search procedures, detectors, and barriers.

Security areas are established when the nature or importance of classified matter or security interests is such that access to them cannot be effectively controlled by other internal measures. Access to security areas is limited to persons who possess an appropriate clearance and have a need-to-know. Access and search controls normally include:

- A personnel identification system
- Positive verification of identity
- A visitor log
- Assessment or search procedures
- Signs indicating that trespassing is prohibited.

A security badge or pass system may be used to ensure that only authorized personnel enter, occupy, or leave a security area, and to indicate the limitations placed on access to classified matter. Badges, passes, and credentials are covered in detail in Section 4 of this guide.

Search systems range from physical and visual search procedures to the use of specialized detection equipment, such as SNM and explosives detectors. Since these systems are heavily dependent on personnel actions, assessors must evaluate the training and capabilities of the individuals operating such equipment. Also, attention must be given to ensuring that search equipment is properly installed. The best trained SPOs, using state-of-the-art equipment, cannot achieve the desired results if the equipment is not properly installed or maintained.

Subjects covered in this section are:

- CCTV identification systems
- Card-reader systems
- Biometric identifiers
- SNM detectors
- Explosive detectors
- Metal detectors (magnetometers)
- X-ray equipment.

A CCTV identification system may be used to provide positive identification of personnel entering security areas as an alternative to protection personnel stationed at the entry point to control access to a security area. CCTV systems allow remotely stationed protective personnel to view a person’s face and identification badge. Equally effective access control measures must be in place at times when the CCTV identification system is inoperable.

Card readers and coded credentials may be used to supplement or replace badge checks as a means of access control. These devices are often used to control access to inner security areas and at facility entry and exit portals. Door locks opened by card readers must be designed to relock after the door has closed to prevent a person from immediately opening the door while it is still in the unlock mode. Card readers at critical locations are usually provided with anti-passback protection. The coded credential technology includes a broad range of applications, including:

- Bar codes
- Wiegand effect
- Magnetic stripe
- Proximity
- Smart cards.

These types of cards normally contain all information required for personal identification.

Biometric identifiers verify personal identity on the basis of some unique physical characteristic, such as eye-retinal pattern, hand geometry, voice, facial recognition, or fingerprints. Retinal scan and hand geometry devices are the most commonly used biometric identifiers at DOE facilities. These devices may be used along with other controls, such as card readers or badge checks. Biometric identifiers are sophisticated devices that require proper installation, regular maintenance, and periodic servicing by authorized manufacturer's representatives.

SNM detectors are used for searching personnel, equipment, or vehicles and help prevent unauthorized removal of SNM. These detectors usually include signal processing and annunciation equipment and are configured as portal, hand-held, or vehicle devices. These detectors must be properly calibrated and sufficiently sensitive to meet site-specific protection objectives as defined in the SSSP.

Explosives detectors may be used for searching personnel, equipment, or vehicles to ensure that explosive components are not introduced into the facility. Protective force or other personnel should be trained for clearing alarms and for taking appropriate actions if a violation is identified. Backup (swipe) detectors must be available at each location where explosives detector portals are in use to resolve portal alarms and for use in the event of portal failure.

Metal detectors may be used for searching personnel to ensure that explosive components, weapons, or other prohibited metal articles are not introduced without authorization. Protective force or other personnel should be trained for clearing alarms and for taking appropriate actions if a violation is identified. Backup detectors (hand-held) must be available at each location where metal detector portals are in use to resolve portal alarms and for use in the event of portal failure.

X-ray machines are also an acceptable means of searching many types of hand-carried items for concealed contraband or other unauthorized material. These machines must be capable of providing a clear picture of objects contained in packages or briefcases. Personnel operating the x-ray machines must be trained to recognize contraband, to take appropriate action when suspected contraband is detected, and to operate the machine and recognize malfunctions.

As the Departmental mission evolves and technology advances, entry and exit assessments will change in scope and rigor. As a result of this evolution, a review of the site's plans for upgrades or equipment replacements is crucial to ensuring that controlled and prohibited items are prevented from being introduced. The assessors should review all current upgrade/replacement projects, as well as future planned projects.

Common Deficiencies/Potential Concerns

Inadequate Monitoring

Inadequate monitoring results when SPOs are inattentive or cannot adequately view the search equipment (e.g., because of poor positioning or post design, or distraction by other duties). Under these conditions, search equipment can be defeated, leading to unauthorized introduction or removal of material.

CCTV Systems

A number of concerns arise when using CCTV identification systems. Since they may be vulnerable to disguise and false credentials, CCTV systems are usually not suitable for high-security areas, such as an MAA. Also, inattention by protective force personnel is a common problem.

Card Reader Systems

A card reader system verifies the coded badge or credential, not the identity of a person. For this reason, these systems are not acceptable as standalone systems for high-security areas and require additional controls, such as:

- Badge checks
- Personal identification number (PIN)
- CCTV identification
- Biometric identification.

Coded credentials are also vulnerable to counterfeiting and decoding. If a lost or stolen badge is not voided in a timely manner, the potential for its unauthorized use increases. Additionally, if the authorized access lists are not updated frequently, persons who no longer have authorization could gain access to a restricted area.

Biometric Identifiers

Facilities have had problems with biometric identifiers frequently rejecting authorized users. At these sites, alternative verification procedures that provide an acceptable level of identification must be available to avoid adverse impacts on the overall protection program. Conversely, some devices are too tolerant; for example, if the band of acceptance is too large, almost any hand, eye, or fingerprint will be accepted.

Retina Scans

Some facilities have had concerns about retina scanning systems where some identifiers are programmed to recognize one eye of the authorized user. Colored contacts lenses, allergies affecting the eyes, or using the non-programmed eye may cause inaccurate results.

Voice Recognition

Voice recognition identifiers are usually equipped with a complementary verbal password to verify authorized users. Users experiencing the common cold or any other change in voice tones usually experience problems accessing the authorized area.

SNM Detectors

SNM detectors are sensitive to the rate of speed at which individuals and vehicles pass through the detectors. For example, if an individual runs through the portal detector or items are thrown through, the detection probability can be substantially reduced. In any case, the SNM detector should be under visual surveillance during operation to prevent attempts to “pass around,” compromise the detector, or otherwise defeat the device.

Explosives Detectors

Explosives detectors are normally sensitive to aromatic, aliphatic, and inorganic compounds, and propellants. They will also detect some non-explosive materials that contain nitrates, such as fertilizers. The speed at which the person moves through the detector is also a concern. For example, if the individual passes through

too quickly, the probability of detection is reduced. For these reasons, the detector should be under visual surveillance during operation to reduce the risk of compromise and circumvention.

Metal Detectors

Metal that is passed through the detector very slowly or rapidly may not be detected. For this reason, procedures are usually in place to monitor personnel and items passing through metal detectors. Personnel assigned to monitor this activity must be properly trained and sufficiently diligent to recognize attempts to defeat metal detection devices. Assessors should pay particular attention to testing of metal detectors at the floor level (in older detectors) because of the metal used in constructing the floor. Metal detectors replaced after 2010 must meet the performance testing procedures and objects cited in National Institute of Justice Standard 0601.02, *Law Enforcement and Corrections Standards and Testing Program*.

X-ray Equipment

X-ray equipment should be examined closely to ensure that it is functioning properly to detect prohibited contraband at the required penetration depths, with sufficient resolution capability to effectively discern prohibited articles. The use of the ASTM standard step wedge with the requirement to image a 26-gauge wire at step five has not been uniformly implemented at all sites.

Planning Activities

During assessment planning activities, assessors interview facility personnel and review available documents. Elements to cover include:

- General policies and criteria for access authorization at each security area. Potential criteria include:
  - Personnel recognition
  - Possession of a badge
  - Possession of a badge and inclusion in a badge exchange system
  - Enrollment in a coded credential system (e.g., card reader) and possession of a coded credential
  - Enrollment in a biometric identification system
  - Possession of a key
  - Knowledge of a combination to a lock or keypad
  - Knowledge of a code word.

- The methods (e.g., badge check, card reader, badge exchange) of verifying the identity of personnel entering each secure area, including:
  - PPA
  - LA
  - Security area
  - Sensitive compartmented information facility (SCIF)
  - Secure communications center
  - Vital Area
  - PA
  - MAA
  - Vault/vault-type room
  - Classified repository.

- Whether more than one method of access control is used at a security area (e.g., badge check and card reader), how the systems complement each other, and which is considered the primary means.

- General methods for determining a visitor's authorization and controlling access.

- Policies and procedures for vehicle control, including volume of traffic and the authorization process for private vehicles, government-owned vehicles, vendor vehicles, emergency vehicles, and SPO vehicles.

- General methods and procedures for conducting entry searches at each security area, especially each PA. (Current technology is not fully effective in searching vehicles for weapons and/or explosives. As a result, major vehicle components must be manually dismantled to be searched thoroughly. Alternatively, vehicles may be escorted by the protective force while they are inside the PA.)

- General methods and procedures for conducting exit searches at each security area, especially each MAA.

- General information about each security area, including:

  - Normal operational hours (e.g., day shift Monday through Friday, or 24 hours a day and 7 days a week)

  - Variations in normal operational hours

  - Approximate number of people assigned to the area

  - Approximate number of people with permanent access authorization to the area (including SPOs, fire squad, and other support groups)

  - Number of personnel portals and approximate throughput

  - Number of vehicle portals and approximate throughput.

Performance Tests

- Personnel Access Control Equipment (Appendix B, Part 1)
- SNM Detectors (Appendix B, Part 2)
- Metal Detectors (Appendix B, Part 3)
- X-ray Equipment (Appendix B, Part 4)
- Auxiliary Power Supplies (Appendix D, Part 1)
- Tamper Protection (Appendix D, Part 2).

Data Collection Activities

Policies and Procedures

A. Assessors should determine whether effective access control policies and procedures are in place. Systems such as personnel recognition, badge requirements, coded credentials and associated card readers, biometric identification systems, key control systems, combination lock or keypad requirements, or other access control measures that are in use should all be addressed.

B. Assessors should determine whether policies and procedures are in place for vehicle control, including private vehicles, government-owned vehicles, vendor vehicles, emergency vehicles, and SPO vehicles. Assessors should determine which vehicles are authorized to enter security areas, how authorization is indicated (for example, sticker pass, government license plate), and how such indicators are requested, issued,

and controlled. Assessors should determine whether procedures are in place to handle special or blanket authorizations for various types of vehicles, such as:

- Protective force
- Fire
- Maintenance
- Ambulance
- Local law enforcement.

Assessors should review the following to determine whether they are complete, current, and consistent with site-specific policies:

- Protective force post orders
- Standard operating procedures
- Health physics policies
- CAS procedures
- Other relevant documents.

C. Assessors should review enrollment and de-enrollment procedures by asking the facility to print the enrollment list for one or more areas and then verify the names on the list by comparing the computer listing to other lists or by interviewing supervisors. Assessors should determine whether all persons on the list are authorized, whether persons who were recently transferred or terminated were removed from the list in a timely manner, and whether the lists are consistent with the information available to SPOs at portals.

D. Assessors should:

- Review search system policies, procedures, and calibration specifications for both personnel and vehicle searches.

- Interview personnel who:

  – Calibrate, test, and maintain search equipment
  – Monitor and respond to alarms (SPOs).

- Determine the length of time SPOs are required to operate detection equipment.

- Tour areas where searches are conducted.

- Review the measures in place that preclude the unauthorized alteration of equipment control settings.

- Evaluate whether ingress/egress points preclude commingling of searched and unsearched personnel.

- Evaluate the implementation of the hand wand metal detector.

- Observe and conduct performance tests on search equipment and procedures to determine whether:

  – Searches are effective.
  – Detection equipment can be bypassed.
  – Detectors and x-ray machines are properly calibrated.
  – Performance test types:

- SNM lead ball shield: Depending on the area, some sites are required to test this source for personnel exiting the facility.

- Metal hand wand and portal detectors:

  - For protective force utilizing the hand wand metal detectors, pre-position the weapon source on an inconspicuous area of the body. Process through the search lane. (Remember, the assessor is verifying the effectiveness of the search equipment and procedures only. Always inform the local security manager of the performance test plan of action.)

  - Ask to use the hand wand to check for rebar or metallic construction material integrated on the floor around the search area.

  - Test all areas of the metal detection portal. Utilize the weapon source by conducting kick and throw-through. Position the weapon source at ankle, waist, and head levels. Introduce a variety of weapon orientations. Document and validate observations.

  - Verify that contraband cannot be passed around the portal. If gaps are observed, initiate a performance test.

- X-ray machine:

  - Conduct a push-through test with a weapon source to determine the clarity of the image on the monitor. Utilize a content bin to assist pushing the weapon source through the x-ray machine area displayed on the monitor (usually just inside the shield curtain).

  - Place the weapon source on top of a larger item, as well as on the sides of the belt and, in some cases, beneath the weighted bin. Look for compressed imaging on the monitor.

  - Some x-ray machines are equipped with anti-push through detectors. Verify and test this feature.

- Determine whether backup search equipment is available (for example, hand-held metal and SNM detectors) and observe the conduct of searches with that equipment.

- Determine the access authorization policies and procedures for visitors, including cleared, uncleared, and foreign national visitors.

- Review:

  - Visit request initiation, processing, and approval
  - Escort requirements
  - Visitor identity verification
  - Visitor access authorization indication (for example, temporary badge, pass, photo identification, temporary card).

- Review automated ECS policies to determine whether they are adequate. The review should include special features of the automated systems and the methods used to deter, detect, or prevent tampering.

- Determine whether individuals controlling access ensure that only persons with proper authorization are admitted and that positive verification of identity is established.

- Determine whether more than one method of access control is used at a security area (for example, badge check and card reader), how the systems complement each other, and which is considered the primary means of access control. Similar to IDSs, these access control systems should be complementary, not supplementary. A full understanding of the controls that are used may enable the assessors to visualize potential problems and means to defeat the controls.

- Determine whether all vehicles, personnel, and hand-carried items entering and exiting MAAs (or PAs encompassing an MAA where Category II SNM is stored outside the MAA) are searched in accordance with DOE requirements. PAs that encompass an MAA but do not have Category II SNM outside the MAA can use random searches of vehicles, personnel, and hand-carried items at a frequency dictated by the cognizant DOE authority. Assessors should also determine whether all items belonging to uncleared personnel going in or out of PAs and MAAs are assessed.

Operations

E. Assessors should observe operations at selected portals to verify compliance with:

- Site-specific procedures
- Personnel and vehicle entry procedures
- Visitor controls
- Personnel and package searches
- Access logs
- Procedures used to place portals in access or secure mode.

During observation of routine portal activities, it is prudent to request (in advance) that the test and maintenance personnel perform their normal testing and calibration activities.

F. Assessors should observe operations at selected storage areas, such as vaults, vault-type rooms, and safes. At these locations, assessors should check entry procedures, including:

- Requests to put alarm systems in access mode

- Lock and double-lock systems

- Entry logs

- Interfaces with protective force or health physics

- The search lane configuration, which includes the protective force (proximity and field of view), monitor and control panel, and entry and exit points on the x-ray machine

- Control methods in the access mode, such as:

  - CCTV
  - SPO posted at door
  - Two-person rule.

- Lockup procedures, including exit searches, lock checks, and procedures to place the alarm system in secure mode.

All of these procedures should be reviewed in light of the possibility of a single insider gaining access to SNM or other security interest. The controls should be structured in such a way that DOE interests are not at risk from a single insider.

G. Assessors should note that except in the case of an emergency response, protective force personnel should not normally be exempt from the requirements for personnel entering certain security areas. Even though protective force personnel are allowed to take authorized weapons and other duty equipment into a security area, they should not be exempt from routine access controls. Such exemption would be an ideal opportunity for the introduction of contraband or unauthorized material into a security area.

Section 4: Badging

General Information

A security badge system is implemented to ensure that only authorized personnel enter, occupy, or leave a security area and to indicate limitations placed on access to SNM and classified matter. To aid in achieving this goal, Homeland Security Presidential Directive 12 (HSPD-12) implemented a mandatory, government-wide standard for secure and reliable forms of identification. HSPD-12 badges should be the primary identification document issued by the Federal government to its employees and contractors, and affiliates requiring long-term access to Federal facilities and information systems. Local Site Specific Only (LSSO) badges (including the DOE Office of Science badges) are also used at specific sites, but only recognized at their issuing site.

Badging systems are normally managed within the facility's security organization. However, the actual badging function is often delegated to other groups at the facility. For example, at some facilities, the protective force issues and controls badges; at other facilities, the employment department may handle some badging functions. At large facilities, a group may be specifically dedicated to badging functions.

How the badge system is implemented varies across DOE facilities, depending on the size and complexity of the site. Sites with only one facility usually have a single office that issues badges, while sites with multiple facilities and/or multiple tenants may have more than one badge office or a centralized badge office with a number of satellite activities that perform the badging functions. Assessors must be aware of such satellite locations, their functions, and their interface with the centralized badge activity.

Most sites use computer-generated badges that have a magnetic stripe coded for access control. SPOs or other security personnel may use these badges as a standalone measure for controlling access to security areas, or in conjunction with a badge check. Although the PSS topic team usually assesses the technical aspects of the coded systems, the personnel security topic team may review procedures for enrolling/deleting personnel in the automated access control system and for issuing and controlling coded badges. Likewise, the cyber security team may review procedures for establishing access controls for the computers that house the automated access control system (e.g., passwords, firewalls). Because computer-generated badges can be duplicated to near-perfect visual and tactile quality, the review of the facility's program for encoding data on the badges is particularly important at facilities that use those badges as a standalone measure to control access to security areas.

The use of integrated systems gives rise to interfaces with badging systems and access control systems. These interfaces constitute a field device network of sorts, which requires protection at the same level as the interests they protect.

Common Deficiencies/Potential Concerns

Improper Badge Accountability Procedures

Records documenting the disposition of all badges may lack the required information: date of issue, description and serial number of badge, organization, destruction date, and name of holder.

Improper Storage of Unused Badging Materials and Unissued Badges

Facilities do not always adequately protect unissued badges against loss, theft, or unauthorized use. Unissued badges may be improperly stored in an unlocked drawer or file cabinet in a badge office or reception area, and left unattended or uncontrolled at times (for example, when the person issuing badges takes a break or leaves to perform other duties). Improper storage can result in the loss of unissued badges and the potential for unauthorized access, which can be a serious problem if the badges are already coded or if a security officer controls access authorization.

Ineffective Badge Recovery and Untimely Access Termination

Badges of terminated employees are not always promptly recovered before their departure from the site. Recovery of badges issued to long-term visitors, student workers, construction workers, or temporary employees can be a particular problem since such persons do not always follow normal termination procedures when leaving the site. Recovery of badges of employees terminated for cause or misconduct and timely revocation of their access via the automated access control system are particularly important to prevent further access to the site and eliminate the possibility of misconduct by disgruntled employees. Assessors should inquire whether there are monetary withholdings or other means to deter individuals, vendors, or the contracting company from retaining expired badges. Assessors should review methods of badge recovery and assess all locations such as drop box repositories, protective force check points, and badge office storage containers to ensure that badges are adequately protected throughout the recovery process.

Improper Badge Destruction

DOE security badges that are deactivated or no longer needed are not always destroyed in such a manner as to ensure that the badge cannot be reconstructed. Assessors should analyze the badge destruction equipment and observe the disposal process to ensure that it is effective.

Failure to Update Badge Photos

If employees do not have a new picture taken when their appearance changes significantly, their badges will not reflect their current appearance. Supervisors, security officials, and protective force officers are responsible for ensuring that the badge pictures are current by reporting to the badging authority any employee exhibiting a significant change in facial appearance.

Incomplete Handling of Lost Badges

When badges are reported as lost, all personnel responsible for controlling access to security areas (usually SPOs) must be informed so that they are able to prevent unauthorized personnel from using the lost badge to gain area access. However, badge offices do not always inform the protective force (or other groups responsible for access control) about lost badges. Even if the protective force is informed, the procedures for getting that information to the security posts or portals may be ineffective or untimely. Procedures for timely deletion of lost badges from the automated access control system and for notifying other organizations about lost badges are a particular problem. Identifying lost badges at portals is rarely effective, since SPOs may not take the time to check the list of lost or stolen badges. Deficiencies in these notifications can lead to unauthorized access.

Insufficient Understanding of Policies and Procedures for All Issued Badges

A lack of understanding of policies and procedures for all types of badges (such as HSPD-12, LSSO, temporary, visitor, and foreign nationals) may be attributable to inadequate training programs or vague, informal, or incomplete procedures.

Insufficient Physical Protection of Field Device Network

The network of devices utilized in the badge-making process should be afforded the same level of protection as the interests they grant access to. Transmission lines may be routed in and out of security areas and may not be given the required level of protection. In some cases, the interconnecting equipment and cabling may not be located in an appropriate security area. These systems may have a remote access capability that can introduce weakness.

Additional examples of insufficient physical protection of badge processing computer terminals and access control databases include:

- Delinquent time scheduled for changing log-on password
- Unauthorized sharing of log-on passwords between personnel
- Exposed USB ports on computer terminal hard drives linked to the general assembly area within the badge office, increasing the potential for unopposed malevolent unauthorized access (e.g., USB ports, inserted key stroke recorder)
- Unsecured badge office processing terminal, badge materials, and equipment during breaks or lunch
- Potential for non-approved personnel to manipulate the access granted and clearance level of badged employee profiles on the database.

Planning Activities

During the planning meeting, assessors should interview points of contact and review available documentation and procedures (for example, SSSPs, personnel security operating procedures, badge system policies, automated access control policies, and visitor control policies) to characterize the badge system policies and implementation. The following elements should be covered:

- A general description of all badging systems and the interface systems used at the facility, including those implemented by the operations office or contractors
- The organizations responsible for managing and implementing badging functions, including:
  - Enrollment/deletion of personnel in the automated access control program
  - Issuance of employee and visitor badges
  - Control and physical protection
  - Accountability of badges and associated inserts
  - Recovery of expired/terminated badges
- Whether any badge offices have satellite offices that may perform badging functions
- General process for issuing non-government vehicle passes into a security boundary
  - Frequency and accountability of vehicle passes
  - Personnel/vehicle correlation
  - Specific requirements for large vehicle access
- Procedures for issuing temporary badges to employees who have forgotten them
- General percentage rate of all Q or L cleared badges issued on site, compared to the reported lost or stolen Q or L cleared badges
- General procedures for obtaining a visitor badge or temporary badge
- General procedures for issuing badges to cleared and uncleared foreign nationals

- General procedures for recovering badges from visitors, temporary employees, and employees who are terminating their employment

- General procedures for escorting uncleared personnel and how escort requirements are displayed on the badge

- General procedures for authorizing foreign nationals

- General methods for protecting badges and records, including:

  - Storage practices (for example, a safe or locked room within an LA)
  - Control when the storage area is unlocked (for example, continuous surveillance)
  - Protection of computerized access control/badging systems

- Accountability systems for badges

- Engineered controls vs. administrative controls for password and availability

- Locations where badging functions are implemented

- General procedures for notifying affected organizations and for taking appropriate action in the automated access control system when a badge is reported lost

- Whether site office surveys that include assessment of badges are available for review, and if so, whether the survey findings were identified and corrected

- Whether the facility has performed any self-assessments of badges (if so, arrange to review the self-assessment reports during the assessment)

- Whether a single authorized badge issuer can process and issue badges that afford access to an area containing SNM or classified matter (there must be a clear separation of duties)

- System diagrams and drawings showing interface points with other systems, such as Human Resources or other badging offices

- Whether specific procedures are in place for enrolling authorized personnel into the DOE human reliability program.

Once the assessors have a basic understanding of the management and implementation of the badge/access control system, they determine which organizations, central badge offices, satellite badge offices, storage areas, and access control locations will be reviewed in more depth during the assessment. At most facilities, all organizations, central badge offices, and access control points can be reviewed. However, at large facilities it is not generally feasible to review every satellite badge office and access point. In such cases, a representative sample may be selected for assessment.

Performance Tests

The performance tests outlined in Appendix E yield data applicable to this subtopic, specifically:

- Badge accountability check (selecting samples of badges and records, and verifying their accuracy)
- Portal badge checks
- Badge issuance.

In addition, assessors may:

- Request to inventory recent expired badges and access control cards.
- Randomly select a few cards and conduct a performance test on a local access control device (ACD) at a security boundary. Many access control cards require a PIN or hand geometry unit to gain access.
- Conduct a performance test on the ACD unit by scanning a valid access control card with an unauthorized hand or PIN.
- Document the data outputs from the ACD readout.
- Team up with the personnel security topic team to cross-reference recently terminated employees.
- Randomly select names and verify that their badges have been recovered and properly deactivated to ensure that the terminated employees cannot gain access to security areas.

Based on the review of the interfaces with this system, an assessment of these locations for appropriate security precautions should be conducted.

In addition to tests conducted by the PSS topic team, any performance tests conducted by the protective force, personnel security, or cyber security teams that involve badge checks or other aspects of the badge system are directly relevant to the PSS topic.

Data Collection Activities

Badge Construction

A. Assessors should examine badges to determine whether the badge design and construction preclude inserting a replacement picture without detectable damage to the badge. Assessors should devote particular attention to temporary badges and visitor badges.

B. Assessors should examine access control cards that are issued to personnel who are authorized to access specific security boundaries. Procedures for card activation and deactivation, as well as processing of lost or stolen cards, should be reviewed.

C. Assessors should examine procedures for issuance and storage of HSPD-12 badges. Assessors should interview managers to determine the timeframe in which the site intends to complete the process of replacing standard badges with HSPD-12 badges. Assessors should also identify any upgrades, enhancements, or modifications to the badge processing equipment and computer database that are related to the changeover.

Documentation and Records

D. Assessors should review badge system policies and procedures to determine whether they are consistent with DOE requirements and whether the implementing procedures are consistent with site-specific policies.

E. Assessors should interview selected personnel responsible for administering the badge/access control system to determine whether the site policies and procedures are implemented as required by DOE orders and as described in site-specific documentation. Assessors should determine whether these individuals understand the purpose of the badge system and their responsibilities concerning issuance, disposition,

storage, and recovery. Assessors may wish to have personnel responsible for the badge/access control system explain each step in the badging process. Assessors should observe these individuals issuing a badge to an employee, a visitor, or a contractor.

F. Assessors should examine the access control/badge disposition records and the record of lost badges for completeness and accuracy. This determination typically involves reviewing a sample of lost-badge records.

Access Control

G. Assessors should interview SPOs who implement badge checks at portals and physically observe or test the portal operations to collect information about how the badge policies and procedures are implemented at the site. Alternatively, the PSS team can coordinate efforts with the protective force, personnel security, and cyber security teams to collect the required information. At selected portals, assessors should attempt to determine whether:

- Post orders relating to badge checks are current and consistent with site policies.
- A copy of the list of lost badges is at the post and includes lost badges of other organizations that are accepted by the facility.
- The SPO is familiar with, and implements, the procedures related to checking the list of lost badges.
- The SPO is familiar with the markings and indicators on the badges.
- The SPO devotes sufficient attention to comparing the person’s face to the photograph.
- The site implements a two-person rule for authorizing access to areas where SNM or classified matter is stored or processed.

In addition, assessors should:

- Ask to inventory recently expired badges and access control cards.
- Randomly select a few cards and conduct a performance test on a local ACD at a security boundary. Many access control cards require a PIN or hand geometry unit to gain access.
- Conduct a performance test on the ACD unit by scanning a valid access control card with an unauthorized hand or PIN.
- Document the data outputs from the ACD readout.

Physical Protection

H. At each badge office selected for review, assessors should determine whether stocks of unissued badges and passes are stored in a way that prevents loss, theft, or unauthorized use. Storage areas, including satellite locations, should be checked to ensure that stocks are adequately protected. Specific information to determine includes:

- The methods for storing the unissued badges (for example, safes, locked filing cabinets, locked rooms).
- Whether the storage repositories are protected by alarm systems or security patrols or both.
- The frequency of protective force patrols during non-operational hours.
- The means of controlling access to the badges or inserts when the repository is open (for example, continuous surveillance).
- Which persons have access to the storage repository or automated access control system (for example, who has the combination to locked safes used to store the badges/inserts, or who has the password to the automated system that encodes the badges) and whether those persons are appropriately cleared and have legitimate need to access the repository/computer. Verify that the badge issuer has a clearance level equivalent to or higher than the badge level issued.
- Based on the protection measures in place (for example, the storage practices, alarms, and patrol frequencies), whether storage meets the requirements as defined in DOE Order 473.3A.
- Whether the field device network between badging stations, Human Resources, and the access control systems is appropriately protected.

Badge Recovery

I. Assessors should review badge records and interview personnel in the badge office to determine whether information associated with employees who are terminating their employment is removed from the automated access control system and whether badges are recovered from them before they leave the site. This can be crosschecked by obtaining, from Human Resources or other appropriate facility departments, a list of employees terminated during a suitable time period (for example, the past three months). The names on the list can then be compared with the automated access control system and badge disposition records to determine whether the badges of these terminated employees were recovered and access was rescinded.

J. Assessors should review visitor logs and badge records and interview personnel in the badge office to determine whether visitors' badges are recovered at the conclusion of the visit. Assessors should determine what actions are taken if a visitor forgets to turn in a badge.

K. Assessors should interview personnel in the badge office and review badge documentation and the automated access control system to determine whether foreign nationals are being appropriately badged (e.g., cleared foreign nationals are issued standard DOE badges with the individual's country of citizenship noted on the bottom of the badge, and uncleared foreign nationals are issued a site-specific badge colored red).

Badge Destruction

L. Assessors should verify that the procedures for and physical aspects of properly destroying expired badges are effective and implemented in a timely manner. Verify that procedures and destruction machines are in place to ensure that badges cannot be reused or information extracted from them. Ask to review the inventory of destroyed badges to verify their effective destruction.

Badge Reissue Requirements

M. Assessors should determine whether employee photos are retaken and badges reissued as required. One way to review this requirement is to observe the badge checks at a portal to determine whether badge photographs accurately reflect the facial appearance of the holder. Another way is to interview supervisors and SPOs to determine their level of awareness of the requirement to report to the badge office any employees who exhibit significant changes in facial appearance. A third method is to review records to determine how many employees have had their photographs retaken in a specified time period (for example, one year). A very small number of retaken photographs may indicate that the requirements are not being followed. If that is the case, the protective force topic team should devote additional attention to portal operations to determine whether personnel have current photographs and whether the SPOs report any discrepancies.

Section 5: Barriers, Locks, and Keys

Barriers control, impede, and deny access and effectively direct the flow of personnel and vehicles through designated portals. Locks and keys help enforce compliance with DOE orders. Therefore, the assessment of barriers, locks, and keys helps determine whether the PSS performs adequately.

5.1 Barriers

General Information

Physical barriers control, impede, or deny access and effectively direct the flow of personnel and vehicles through designated portals. The evaluation of barrier system effectiveness is based on whether the system complies with DOE orders and whether performance testing indicates that it performs adequately. Specifically, barriers are designed to:

- Reduce the number of entry and exit paths
- Facilitate effective use of protective force personnel
- Delay the adversary to enable assessment and protective force response
- Protect personnel from hostile actions
- Channel adversaries into pre-planned neutralization zones
- Prevent stand-off attacks from vehicle-borne improvised explosive devices
- Establish concentric security area boundaries for PPAs, LAs, PAs, MAAs, and vaults.

The following subject areas are addressed in this section:

- Fences
- PIDAS barriers
- Buildings
- Doors
- Security containers
- Denial systems
- Vehicle barriers
- Active denial systems.

Fencing is normally used to enclose security areas and to designate DOE property boundaries. Depending on the intended level of security, fences require regular patrols, continuous observation, or an IDS supported by alarm assessment equipment. DOE requires that fences:

- Meet specific gauge and fabric specifications
- Be topped with particular wire and outrigger configurations
- Include steel posts with bracing
- Meet certain height and location provisions.

Buildings of various types represent the most common barrier used to protect DOE security interests. Construction features vary throughout the DOE complex. However, a number of basic requirements must be considered when evaluating the walls, ceilings, and floors that enclose security areas. In general, building materials should be solid and offer penetration resistance to, and evidence of, unauthorized entry. DOE orders and manuals provide requirements for a variety of construction elements, including:

- Wire mesh
- Insert panels
- Sound attenuation for rooms in which classified information is to be discussed
- Storage rooms.

There are also specifications for construction hardware. For example, with the exception of fencing, all hardware accessible from the outside is required to be peened, brazed, or spot-welded to preclude tampering or removal.

In addition to the criteria for walls, ceilings, and floors, there are requisite construction requirements for doors, windows, and unattended openings. Doors should offer resistance to forced entry. When necessary, reinforcement is required for doorjambs, louvers, and baffle plates. Windows, when relied on as physical barriers, must be constructed of shatter-resistant, laminated glass of a minimum thickness and installed in fixed frames so that the panes are not removable from the outside. Window frames should be securely anchored in the walls and locked from the inside. Unattended openings larger than 96 square inches should be alarmed or equipped with steel bars. When properly installed, steel bars will reduce the size of the opening. In addition to construction requirements, there are requirements for penetrations of security area barriers. Elevators that penetrate a security area barrier should have an access control system that meets the access control requirements for the security area being penetrated. Utility corridors that penetrate security area barriers must provide the same degree of penetration resistance as the barriers they penetrate. Objects that intruders could use to scale or bridge barriers and enter security areas must be removed or secured to prevent their unauthorized use. If a security area configuration is altered, barriers must be erected (e.g., during construction or temporary activities), and at a minimum, a risk assessment must be conducted to validate equivalent protection measures. A barrier design must consider proximity to buildings or overhanging structures.

The General Services Administration (GSA) establishes standards for security containers. Although classification is the only security factor that determines the degree of protection required for classified matter in storage, other considerations include:

- Strategic importance
- Susceptibility to compromise
- Effect on vital production
- Health and safety
- Replacement costs.

Other DOE requirements address:

- Protective force assessments and patrols
- Transfer of security containers
- Protection of security containers and combinations
- Security repository information
- Repair of containers.

Active denial systems include cold smoke, carbon dioxide, and other dispersible materials such as sticky foam, rigid foam, sprays, and irritant agents. These substances should be properly maintained and protected against tampering. Other systems may incorporate flickering light or intense sound systems to delay, confuse, or otherwise hamper adversaries.

Passive denial systems include building structures (for example, walls, doors, floors, ceilings, and windows), security bars, and large natural or manmade objects (for example, large boulders or concrete blocks). The mechanism for moving or disengaging passive systems should be protected at the same level as the interests they protect.

Vehicle barriers are used to deter penetration into security areas when such access cannot otherwise be controlled. Vehicle barriers may include pop-up barriers, cables, bollard configurations, or natural terrain obstacles (for example, bodies of water, ravines, tank traps, ditches, Jersey barriers, steep hills, or cliffs).

Common Deficiencies/Potential Concerns

Fences

To be effective, fencing must be checked and repaired on a regular basis. Frequently, the fence fabric is not properly attached to the support poles and the bottom wire is not secure. Erosion of the ground under the fence can produce gaps or washouts that may allow someone to crawl under the fence. Another common problem is that vegetation is allowed to grow up close to the fence, potentially providing concealment for adversaries or a platform for climbing over the fence. Fences should be installed no closer than 20 feet (6 meters) from the building or the safeguards and security interest being protected.

PIDAS Barriers

The following barriers may or may not be positioned in an effective location with respect to the PIDAS. Additionally, the barriers may not be secured adequately to perform their purpose:

- Aerial screens/netting – These may not be effective in preventing specific classified objects that are located at that site from being thrown over fencing or alarm detection zones.

- Parking blocks located in alarm detection zones – These may not be configured effectively to prevent adversaries from crawling beneath the IDS coverage area.

- Aircraft cables – Cable tension points may be accessible, allowing the cable to be severed and dropped to ground level.

- Bollards/removable bollards – These may not be securely fastened or may be spaced too far apart, allowing small vehicles unimpeded access into security areas.

- Jersey barriers – These may not be configured effectively to reduce the speed of vehicles approaching a security area.

- Concertina wire/razor ribbon – PIDAS camera towers/or other fixed structures and fence-break points may lack sufficient coils to impede stealthy or forcible entry into the security area.

Buildings

Suspended ceilings and raised floors often create the illusion that they represent the “hard” surfaces of the enclosed space, and assessors can easily overlook these configurations. The ceiling and floor panels must be assessed to ensure that the true “hard” walls and surfaces of the building are identified, especially in locations where PA, MAA, vault or vault-type room, or SCIF boundaries are established.

Doors

An astragal or mullion must be used where double doors meet to prevent the insertion of breaching tools. Door louvers and baffles must be reinforced to preclude their removal from outside the area being protected.

Security Containers

Some facilities have requested and received exceptions for the use of non-GSA-approved containers for storing classified documents. Assessors should not assume that all facilities have these exceptions. All exceptions received by the assessed facility should be reviewed before the onsite assessment to determine whether they are current.

Denial Systems

Some DOE facilities use a form of denial system that consists of an extremely heavy block of concrete placed in front of an access door to protect critical assets. To gain access, a hydraulic vehicle or some other lifting mechanism must be used to move these barriers. Since these vehicles or mechanisms are critical to the effective application of this kind of barrier, they must be afforded an appropriate level of protection. Assessors should check to ensure that these items of equipment are appropriately protected and properly maintained.

Vehicle Barriers

Vehicle barriers must be effectively monitored, and components must be appropriately located. Barriers should be within an area that is protected by detection sensors. Controls for vehicle barriers and motorized gates that are used at entry control points must be located within protective force posts or other locations as described in the SSSP. Additionally, any associated hydraulic and mechanical systems must be protected from potential sabotage.

Active Denial Systems

Adequate measures must be provided to prevent an insider from disabling active denial systems (such as cold smoke or sticky foam). Since most such systems have a single location for firing, that location is vulnerable to insiders unless sufficient protective measures are applied.

Planning Activities

During the planning meeting, assessors should interview facility personnel and review available documentation relative to the presence and use of barriers. This documentation should include building construction drawings, focusing on barrier construction details and heating, ventilation, and air conditioning ducts. Elements to cover include:

- The general types of barrier systems (e.g., fences, standard building materials, reinforced/hardened building materials) in place at each secure area, including:
  - PPA
  - LA
  - Security area
  - SCIF
  - Secure communications center
  - PA
  - MAA
- The types of barrier systems associated with the various storage/process areas (e.g., vaults, safes, vault-type rooms) used to protect SNM and classified matter. In particular, determine:

- Whether active denial systems (e.g., smoke, foam) are used
- Whether items within storage areas (e.g., vaults) are protected by additional controls (e.g., locked compartments, tie-downs)
- Methods for providing delay when material is in use and when storage areas are in the access mode
- Interfaces that may exist between ECSs and IDSs
- Whether airborne denial systems are in place in any areas

- The types and locations of vehicle barrier systems.

Performance Tests

No performance tests are directly relevant to this subtopic. The use of performance test results to identify delay times is discussed under Delay Time, below.

Data Collection Activities

General

A. Assessors should determine whether barriers at facilities with Category I SNM or classified matter provide sufficient delay to allow the protective force to assess alarms and respond with sufficient force to neutralize the adversaries before they have completed their intended purpose. (This evaluation is generally based in part upon on a review of VAs.)

B. Assessors should determine whether barriers are sufficient to ensure that SNM cannot be removed from the area without causing an alarm or immediate visual evidence of tampering. Also, assessors should determine whether barriers are sufficient to channel personnel through designated portals or into adversary neutralization zones.

Perimeter Barriers

C. For security areas where a perimeter barrier system is used, assessors should determine what types of barriers are in use (for example, fences, wire, vehicle barriers, or natural obstacles), whether they meet DOE requirements, and whether all barriers are accurately represented in VAs and in the SSSP. Assessors should determine whether procedures are in place to prevent transferring contraband or SNM over an exterior perimeter barrier (for example, throwing or slinging items over a fence for later pickup). Preventive measures may include wide isolation zones, extra-high fences or nets, or adequate surveillance by protective force personnel. Barrier placement should be evaluated to ensure that the critical protective force field of view is not compromised, and to ensure that an attacking force is not provided a tactical advantage by utilizing the barriers for cover.

D. Assessors should examine fences to determine whether their condition would allow adversaries to get through or bypass them without being detected. Some items to consider include:

- Erosion in isolation zones or under fences that may allow an adversary to pass undetected
- Unprotected pipes or wires that pass over fences or other perimeter barriers and allow an adversary to pass over the barrier

- Inadequately protected tunnels, underpasses, culverts, or pipelines that pass under the perimeter barriers

- Adjacent structures in close proximity to either side of the fence that could facilitate bridging.

Buildings

E. Assessors should determine whether construction materials are sufficient to provide appropriate delay against a number of adversary penetration methods, including hand tools, power tools, and explosives.

F. Assessors should visually assess vaults, vault-type rooms, and vault construction diagrams to verify whether the construction requirements comply with DOE orders.

G. Assessors should verify whether the construction requirements for security containers comply with applicable DOE orders.

H. Assessors should be prepared to conduct a thorough examination of a building. If only a portion of the building is a security area, assessors should be prepared to tour the security area perimeter. It may be helpful to carry building floor plans. Other areas that should be checked include:

- Air ducts
- Electrical conduit and pipe penetrations
- Storage areas
- Walls
- Windows
- False ceilings
- Underground pathways.

I. Assessors should review fixed barriers that shield protective force personnel (for example, towers, portals, alarm stations, and defensive positions) to determine whether they meet the requirements of DOE orders. Reviewing documents, interviewing security staff, or conducting visual assessments may accomplish this. For posts constructed after 1985 designed to protect SNM (Category I or II), exterior walls, windows, and doors must provide bullet resistance equal to the "high-power rifle" rating of Underwriters Laboratory 752. Assessors should look for a marking or stamp on the window or structure that indicates "high-power rifle," or Level 8, protection. Assessors should also determine whether procedures are in place to preclude protective force personnel stationed within these posts from activities that could negate the purpose of these hardened posts.

J. Assessors should review the design of vehicle barriers to determine whether they meet DOE standards in accordance with the applicable Graded Security Protection Policy. To make this determination, assessors may need to interview the responsible engineers, review vendor data, or review test results. Assessors should also review barrier operational procedures to ensure that they are effectively integrated into the protection strategy. Barriers left in the "down" position until identification of a potential threat or during a heightened security event do not prevent penetration by a malevolent vehicle during normal operations. Additionally, if credit is taken for emergency "up" operation of the barrier in the production strategy, testing should be performed to determine whether the speed of barrier activation is adequate to address the Graded Security Protection Policy.

K. Assessors should review active denial systems to determine the effectiveness of their activation methods and the conditions and procedures for activation. These systems should be examined to determine whether they are properly installed and in good condition, have effective power and backup power sources, and are tamper-resistant. The operator's familiarity with system activation should also be checked.

Delay Time

L. Assessors should review documents, interview security staff, review as-built designs, and visually assess barriers to determine the delay times the facility has estimated for various barriers. These estimates should be reviewed to determine whether they are credible and whether protection is balanced. (For example, a vault door used in a room with transite walls is a case of inappropriate protection, since one barrier is significantly more vulnerable than the other.) Assessors can also compare delay time estimates with response times and response procedures to determine whether response plans are effective and give appropriate consideration to the physical security hardware.

Guidelines for identifying penetration times by reviewing site-specific documents are:

- SSSPs should contain parameters related to barrier delay times or to the minimum delay times required to ensure an effective response. Such delay times may relate to individual components (such as doors) or to the total delay time involved in reaching a target or performing an action. However, most SSSPs do not provide this level of detail. Instead, they usually reference a site security plan or VA that may include delay time information.

- SSSPs may describe barriers, including doors and adjacent barriers. These descriptions may include penetration times for individual barriers or may reference the data source.

- VAs may contain penetration times for individual barriers in one or more locations. The narrative may address individual barriers and may include delay times. Also, computer codes are frequently used to conduct the VA, and the input to these codes frequently includes delay times. For example, the Analytical System and Software for Evaluating Safeguards and Security (ASSESS) or Adversary Timeline Analysis System (ATAS) codes are frequently used when developing VAs at DOE facilities. The input includes delay times for portal entry doors, exit doors, and surfaces. When reviewing computer input to determine the penetration times assumed by the facility, the following points should be considered:

  - The input delay times may be different for different facilities or for different scenarios.

  - The input delay times may assume that the door is secure, but there may be scenarios where the door is open or in access mode.

  - If several barriers are in a series, the delay times may be added if the adversaries must pass all barriers sequentially to reach a target.

- System requirement documents or design specification documents are an excellent source for determining expected penetration times. Unfortunately, such documents are not always available or are difficult to find. If these documents are available, the responsible security engineering group is the most likely source.

- Penetration times for doors and adjacent barriers can be significantly affected by a number of factors, including the mode and timing of the adversary attack and the adversary's level of sophistication.

Guidelines for visually assessing barriers and reviewing as-built diagrams are:

- The construction and materials used in barriers can usually be determined by visual assessment or by a careful review of as-built diagrams. With this information, assessors can generally make a rough estimate of penetration resistance. The Sandia Access Delay Technology Transfer Manual and other security design manuals may be useful for this purpose.

- During a visual assessment, the assessors should focus on barrier deficiencies or design flaws that an outsider could exploit. These include flaws that would allow surreptitious penetration of the barrier, penetration in less time than estimated (e.g., with an insider's help), or defeat of the protection element, as well as flaws that could allow an insider to assist an outside force.

Guidelines for gathering information on penetration times by interviewing security staff or engineers are:

- Discussions with the security personnel who conducted the VAs or who are responsible for barrier design may be useful for reviewing site-specific documents.

- If penetration times have been documented, assessors should interview knowledgeable security personnel to determine how penetration times were developed, what assumptions were made, what modes of attack were considered, and what adversary threat characteristics were assumed.

- If penetration times have not been documented, assessors should interview knowledgeable security personnel to gather information on the effectiveness of the barrier design. Potential discussion topics include:

  – Alarm response procedures (in particular, the sufficiency of response time in terms of barrier design)
  – Whether penetration resistance was factored into response plans
  – Design and construction (materials used, use of tamper-resistant hardware, hardening of barriers as part of an upgrade program).

General guidelines for using performance test results to identify delay times are:

- EA may occasionally conduct performance tests of barriers to determine penetration times.

- Tests involving a significant potential for personal injury (for example, crawling through razor ribbon) are not conducted.

- The types of tests for penetration times that assessors would typically conduct are simple ones designed to demonstrate potential vulnerabilities. For example, an assessor may conduct a simple test of an adversary's ability to defeat a steel-grate door that has a crash bar on the inside; such a test might involve inserting a bent rod through the steel grate to engage the crash bar. Such tests may demonstrate that the assumed delay times did not consider all credible modes of attack.

- Assessors may identify penetration times by reviewing the results of tests on similar barriers that the facility, other DOE elements, or outside agencies conducted. Frequently, facilities conduct (or contract others to conduct) tests of barriers prior to installation. Also, vendors often have penetration time results for selected modes of attack. However, test results should be reviewed critically, with particular attention to:

  – How the penetration times were determined
  – The modes of attack considered
  – The level of adversary sophistication
  – The type of results reported.

Other general guidelines to be aware of when dealing with penetration times are:

- Penetration times are significantly influenced by the mode of attack. For example, hardened doors that would take several minutes to penetrate with power tools frequently can be breached via explosives in less than one minute. Assessors should review the data and determine whether the modes of attack that the site has considered are consistent with the parameters of the approved threat guidance.

- A well-placed insider can defeat most barriers. For example, an insider can open a door from the inside and allow adversaries to enter, reducing the delay provided by the door. Assessors should look for design features that would make a barrier particularly susceptible to defeat. Assessors should also look for key insiders who are in a position to defeat multiple layers of protection. The assessment team should identify other protection measures in place to prevent insider tampering (for example, protective force patrols). The fact that well-placed insiders can defeat a barrier does not necessarily make that barrier inadequate, since multiple layers of protection should be afforded to SNM. The potential actions of an insider need to be examined in a broader context and considered in light of multiple layers of protection and the parameters of the SSSP.

- Penetration time estimates are not precise values. Consequently, any comparison of penetration times is a rough comparison. The intent is to determine whether the protection is reasonably balanced and whether the barriers provide sufficient delay to allow effective response. For example, if the penetration time of a door is 1.5 minutes, whereas the penetration time of the adjacent wall is 2 minutes, this will not normally be cause for concern (assuming that the overall delay time is sufficient to allow an effective response). However, if a Class 5 vault door is installed in a transite wall, this would clearly indicate unbalanced protection. One reference used throughout the DOE community is the Sandia Access Delay Technology Transfer Manual.

5.2 Locks and Keys

General Information

Locks are an integral part of the physical barrier system and are used to control, impede, or deny access and to effectively direct the flow of personnel and vehicles through designated portals. The effectiveness of security locks is based on compliance with DOE orders and whether performance testing indicates that the system performs adequately. The requirements for security locks are determined in light of the security interest being protected, the identified threat, existing barriers, and other protection measures.

Specifically, locks are designed to:

- Reduce the number of entry and exit paths
- Keep unauthorized personnel from entering areas where they are not allowed
- Control access to assets within areas to individuals with an approved need.

Security keys include electrical and mechanical technologies, key cards, and other non-standard locking type devices. Security keys do not include administrative or privacy lock keys for factory-installed file cabinet locks, desk locks, toolboxes, etc. Because keys are easily lost or duplicated, a strict key control program must be developed, implemented, and effectively managed to ensure continuous accountability of security keys.

The following subject areas are addressed in this section:

- Types of locks and specifications
- Levels of protection and requirements
- Storage requirements for locks and keys
- Lock and key control management.

The officially designated security authority (ODSA) must establish a program to protect and manage locks and keys, and the requirements for security locks must be applied in a graded manner. Locks used to protect classified matter and Category I and II SNM in GSA-approved security containers, vaults, or vault-type rooms must meet Federal specifications (see Federal Specification FF-L-2740A Amendment 1, Locks, Combination). Key locksets

must meet American National Standards Institute (ANSI) Standard A156.2-1996, Grade 1, *Bored and Preassembled Locks and Latches*, or ANSI A156.13-1996, Grade 1, *Mortise Locksets.* DOE Order 473.3A provides other specific requirements for these locksets.

Combination padlocks must meet Federal Specification FF-P-110J, *Padlock, Changeable Combination*, and standards cited in 41 Code of Federal Regulations (CFR) Part 101, *Federal Property Management Regulations*.

Security key padlocks must meet the following specifications:

1. Security key padlocks that are considered "high security" must be shrouded-shackle and key-operated and must meet standards in MIL-P-43607H, *Padlock, Key Operated, High Security, Shrouded Shackle.* High security padlocks, approved to secure Category I and II SNM and Top Secret and/or Secret matter, are identified as Level I.

2. Low security, regular (open-shackle, key-operated padlocks) must meet the classes and standards in Commercial Item Description A-A-59486B and A-A-59487B. The ODSA must determine low security padlock usage based on the site analysis of the security interest being protected.

   Hasps and yokes on containers storing classified matter must be constructed of steel material, at least ¼ inch (6.35 millimeters) in diameter or equivalent cross section, and secured to the container by welding or riveting to preclude removal.

   General field service padlocks are heavy-duty, open-shackle locks that meet Federal Specification FF-P-2827A Notice 1. The key-operated padlocks are designed to withstand exposure to grit and corrosive or freezing environments. The ODSA must determine general field service padlock usage based on the site analysis of the security interest being protected.

Security keys, key blanks, and key cutting codes must be protected in a graded manner. The same protection considerations that apply to keys also apply to locks, i.e., the interest being protected, the identified threat, existing barriers, and other protection measures afforded the asset.

Security locks and keys are divided into four levels, Level I through IV, based on the site analysis of the security interest being protected. The ODSA must determine the appropriate level for application to the site. Facilities that do not possess nuclear weapons, weapon components, SNM, classified matter, or high value government property should follow the requirements established for Level III and Level IV locks and keys.

- Level I locks and keys are used to protect nuclear weapons, weapon components, Category I SNM, Category II SNM that rolls up to a Category I quantity, certain high value government assets, and Top Secret and/or Secret classified matter. Security key blanks must be restricted/proprietary and unique to the site. Security locations, such as vaults, vault-type rooms, MAAs, SCIFs, and security areas where Top Secret and/or Secret documents are stored, require Level I security locks and keys (see DOE Order 473.3A for other specific requirements).

- Level II security locks and keys are used for building doors, entry control points, gates in PA fences, and security area doors or other barriers or containers that protect Category II and Category III SNM and classified matter, including documents classified at the Confidential level.

- Level III security locks and keys are used on buildings, gates in fences, cargo containers, and storage areas for protecting Category IV SNM, and on government property where loss would adversely impact security and/or site/facility operations.

- Level IV locks and keys are typically used for offices where there is no storage of classified material or SNM.

Administrative keys, which include desk keys, keys to office supply cabinets, and vehicle keys, are not considered security keys and have no specific control or accountability requirements. Keys to certain vehicles identified in the site's VA as a particular security concern will require added protection. Security locks and keys must be stored in a manner that prevents loss, theft, or unauthorized use. Level I locks and keys, once put into service inside a PA, must not leave the PA without authorization or are considered unaccounted for and must be reported as lost. Assembled security locks or cores and Level I security keys must remain under the direct control of a responsible person or must be stored in a GSA-approved repository or vault-type room. Level I keys must be isolated from all other keys on tamper-resistant, serial-numbered key rings and in key storage cabinets. Keys to storage cabinets must be in the physical possession of an authorized person or locked in a GSA-approved repository. In order to implement corrective actions immediately after an incident involving the loss, theft, or destruction of a Level I lock or key, a risk assessment and compensatory measures must be pre-established and documented.

Level II locks and keys, once put into service, must not leave the facility without ODSA approval.

Locks and keys are categorized according to the asset being protected. An inventory and accountability system must be implemented to ensure the accountability of Levels I, II, and III security locks, keys, key rings, key ways, and pinned cores.

The inventory system must be approved by the ODSA and documented in the S&SP. The inventory system must track the fabrication, issuance, return, replacement, and/or destruction of all Level I, II, and III security locks and keys:

1. Duplicate and replacement keys must not be assigned the same key number as the key being replaced or duplicated.

2. Inventory records must also include sufficient detail to identify locks and keys in possession of individual custodians, issuance stock, and keys assigned to key rings/key cabinets. The inventory record must include the list of the locations of locks that each key will open.

For Level I locks and keys, a 100 percent inventory must be performed semi-annually by the responsible organization.

For Level II and III locks and keys, a 100 percent inventory must be performed annually. Level IV locks and keys have no requirements for control and accountability.

Level IV locks and keys have no inventory requirement.

The number of Level I and II keys must be kept to an operational minimum.

Key rings for Level I and II must have a unique identifying number placed on the ring.

When a Level I security key is unaccounted for, immediate notification must be made to the ODSA, compensatory measures must be immediately initiated, and an incident of security concern inquiry must be completed. If the key cannot be located within 24 hours, the affected lock must be changed.

All parts of broken Level I, II, and III security keys should be recovered. If the functional part (the blade) of a Level I or II key is lost or not retrievable, it must be reported as a lost/missing key. If the blade of a Level III key is lost or not retrievable, it must be reported to the ODSA.

Obsolete, damaged, or inoperative Level I, II, and III keys must be destroyed in a manner authorized by the ODSA and the destruction recorded.

Common Deficiencies/Potential Concerns

Many locks used for security purposes are advertised as "high-security" or "medium-security" locks. However, when examined, these lock specifications often do not meet the required military standards or DOE requirements. Assessors should be aware that the terms "high security" and "medium security," when used commercially, may not have the same implication as they do in DOE orders.

Effective control must be maintained to ensure that locks and keys are used appropriately. Combinations must be changed at specified times and under specified conditions, and key control procedures must be documented and followed. Appropriate procedures for dealing with lost keys must be established. Additionally, when keys are lost, stolen, or otherwise unaccounted for, proper reporting must be completed according to the DOE order that applies to reporting incidents of security concern.

Other common deficiencies in the lock and key program occur when custodians do not maintain an effective accountability system for security keys and allow obsolete or unusable keys to accumulate without taking appropriate destruction action. Assessors should review inventory records to ensure "cradle to grave" accountability for security keys and an adequate destruction process. Assessors should also review the organization's self-assessment program to ensure that it adequately addresses the lock and key control program. Additionally, DOE site office survey programs should include the lock and key programs in their annual surveys of contractor organizations.

Planning Activities

The objective for organizations is to reduce the number of keys and move toward a keyless access control technology. This new effort would help ensure prevention of access to any single physical item or object that can be lost or stolen. Assessors should review plans proposed or in process at each site and DOE site office to determine the status of this initiative. Recognizing that this is a long-term initiative, assessors need to review the existing lock and key programs to determine the effectiveness of the system that is in place.

Assessors should review the key control system to determine whether procedures are in place to adequately control keys and locks. Typically, an effective key control system includes procedures that address control and accounting for keys and locksets (including issue, sign-out, inventory, destruction, and the key and lock numbering system), and procedures used when a key is unaccounted for. The following factors may also be included:

- Criteria for issuing a key or combination to a person (for example, supervisors developing authorized lists and notifying locksmiths in writing)
- Procedures for changing lock combinations (for example, when a person possessing a combination transfers, resigns, is dismissed, or no longer requires access)
- Procedures for using and protecting combinations for Level 1 "A/B" locks by an authorized custodian (for example, administrative controls deterring a person from carrying a classified combination on their person to assist in remembering the combination to open a Level 1 lock)
- Procedures and conditions for changing key locks or lock cores
- Procedures for returning keys when personnel or programs are terminated or when an individual no longer needs the key
- Procedures for conducting and documenting an assessment of duties for possible enrollment of locksmith personnel into the DOE human reliability program (10 CFR Part 712).

Assessors should visit the lock shop and interview the locksmith to determine the adequacy of methods used to protect keying and core information. The following factors should also be considered:

- Procedures for notifying the locksmith that locks or combinations need to be changed, and the time required to accomplish these changes. Assessors may identify these items by reviewing records. For example, when locks are changed because of a lost key, assessors should be able to locate the records indicating when the key was reported lost, when the custodian reported the loss to the locksmith, when a work order was issued, and when the work was completed.
- Methods for numbering keys and locks, and whether the numbering methods unwittingly reveal information about the master-keyed system.
- Procedures for periodically changing combinations and lock cores.
- Procedures for maintaining locks, particularly locks that are exposed to severe weather conditions.
- Procedures for documenting any installation, replacement, or maintenance activities associated with Level I security locks, including the name of the person who performed the activity.

Performance Tests

Performance tests validate the effectiveness of implemented requirements, and assessors should conduct performance testing of the lock and key program as necessary. The following performance tests are not inclusive. Assessors should develop and conduct other performance tests as appropriate.

Required

- Verify accountability of 100 percent of Level I keys. Each of these keys must be physically touched by the assessor and its stamped serial number checked.
- Determine whether issued Level I keys are or have been removed from the PA without authorization.
- Ensure that key rings containing Level I keys have tamper-indicating features and that a unique identifying number is placed on the ring.
- Confirm that Level I key rings do not include any Level II, III, IV, or administrative keys on same ring.
- Verify that lock and key custodian inventory lists are up to date and accurately identify the location of all security keys.

Suggested

- Randomly select Level II keys using lock and key records. Physically locate the keys to determine whether they are or have been removed from the facility without authorization.
- Randomly select Level III keys using lock and key records and physically locate the keys to verify accountability.
- Randomly select Level IV keys using lock and key records. Physically verify that these keys only access offices where no government assets are located and no classified matter or SNM is stored.

Data Collection Activities

A. Assessors should determine whether the organization is moving forward on the keyless access control initiative by reviewing project plans, budget documentation, milestones, etc. Assessors should also determine the effectiveness of the existing lock and key control program by gathering data to answer the following questions:

- Have locks and keys been correctly characterized using a graded approach based on the asset being protected?
- Are locks, keys, and other ACDs protected according to DOE Order 473.3A?
- Have procedures been developed and implemented that define the administration and management of the lock and key program, including roles and responsibilities?
- Has an effective incident reporting system been developed that includes lost, stolen, and unaccounted for Level I, II, and III keys?
- Is the number of keys and ACDs maintained at the absolute minimum required for mission completion?
- Is the number of master keys strictly limited, and are they adequately controlled?
- Are keys restricted from leaving security areas and facilities as required by DOE Order 473.3A?
- Are all keys accounted for, and is a current inventory on file?
- Is lock and key control management included in the contractor self-assessment program and the site office survey program?
- Is there strict accountability of keys using either an automated or hardcopy issuance record?
- Has an effective database been developed to account for and track all Level I, II, and III keys?
- Do Level I locks have restricted/proprietary key blanks? Are they unique to the site, or do they use commercially available master key blanks?
- Are the cutting and pinning of Level I locks and keys done on site in an approved LA, or off site? If done off site, are the Level I key codes at risk of compromise during this process?
- Do administrative keys to any site vehicles that are identified in the facility's VA receive additional protection above and beyond standard administrative keys?

Section 6: Communications

General Information

PSS cannot operate independently of the human element, and a method for communicating quickly, clearly, and reliably must be established. Telephone, radio, and duress alarms provide the necessary communication links among the alarm stations, mobile and fixed posts, response forces, and local law enforcement agencies (LLEAs). The effectiveness of communications equipment is based on compliance with DOE orders and performance during equipment testing and performance tests. DOE policy requires that communications equipment allow the effective protection of safeguards and security interests by providing rapid, reliable, and protected information exchange between onsite protective personnel and the CAS and SAS.

The design of communication systems must be such that no single event can disable all modes of communication between the alarm stations and fixed posts or between the alarm stations and LLEAs. Communications equipment and systems are required to be tested daily for operability, and alternate communications capabilities must be available immediately upon failure of the primary system. Records of the failure and repair of all communications equipment are required to be maintained in a form suitable for compilation by type of failure, unit serial number, and equipment type.

The following subjects are covered in this section:

- Radios
- Telephones
- Duress alarms
- Intercoms, public address, pagers
- Audio recording systems.

Radios are used for voice communications among members of the protective force and alarm stations, and with DOE managers and other participants, when required. Additionally, radios are used to communicate with LLEAs who participate in exercises or respond to emergencies. To provide the flexibility necessary for all participants who may need radio communication capability, a number of frequencies must be available, especially during emergency conditions. For example, one frequency can be used for members of the protective force, one for special response teams (SRTs), and one for communicating with LLEAs. Since most sites are transitioning to trunked or simulcast radio systems, the number of frequencies is increasingly more important. However, the priority levels associated with the talk groups is of greater concern than the number of frequency pairs. Although DOE policy requires dedicated channels in trunked and simulcast systems, dedicating frequency pairs is not technically possible. Features are available that can give security-related communications priority over other users, commonly referred to as "ruthless preemption." It allows specific talk groups to interrupt other users on the radio network. This feature must be taken into account when looking at newer systems. Also, radios must be readily available in sufficient quantities for protective force personnel to perform their duties.

When repeaters are used to increase radio communications range and clarity, these devices (antennas and other exterior components) should be protected from tampering and sabotage. Also, a radio system needs an effective preventive maintenance program in place to ensure that radios and radio components remain functional.

Although alarm stations and radio communication centers should have radio and telephone channels of communication with LLEAs, the telephone is normally the primary means of communication between protective forces and LLEAs, and between the site and DOE Headquarters or the DOE Emergency Operations Center (EOC).

Telephone systems are the primary means of communication at most DOE facilities. Although the telephone is often taken for granted, the telephone system used for security purposes should be protected (alarmed, buried

cable, or line in a conduit) and have backup provisions, especially when used for direct-line communication between the CAS/SAS and guard posts. A good preventive maintenance system should be in place to ensure that the system remains reliable and operates at peak performance. Additionally, cellular telephone technologies are being implemented at some sites. Because the site does not own or have any control over the cellular network they are connecting to, the use of these systems needs to be evaluated. Further, since these systems are often used as the backup or alternative to radio broadcasts, it is important to observe these systems in use during emergency situations, such as force-on-force exercises.

Duress alarms are primarily used to alert protective forces to emergency or duress conditions. The alarm must be activated in an unobtrusive manner and must not annunciate at the post initiating the alarm. Usually these alarms are hardwired devices that are protected from tampering. Radios also may include a duress feature. All duress systems should have procedures in place that provide for maintenance and testing to ensure that they remain in good working condition.

Intercommunication (intercom) and public address systems are normally used to provide information or instructions to selected organizations or individuals, or to the general facility population. Pagers and/or cellular phones may be used for contacting individuals or sending messages, and they are often issued to key security, safety, and management personnel who must be notified in case of an emergency. All of these devices are especially important during emergency situations when speed is critical and when instructions must be disseminated to as many people as possible.

A continuous electronic recording system is used to record all security radio traffic, including all protective force radio transmissions and duress alarms, and transmissions going into and out of the CAS or operations center. Sometimes, telephone conversations conducted over security channels are also recorded.

Common Deficiencies/Potential Concerns

Radios

Although radios are required to provide a multichannel capability, some radio systems used at DOE sites do not have enough channels (radio frequencies) available to provide effective communications for all who need to use the radio. If too few frequencies are available, the primary frequency becomes cluttered with radio traffic. As a result, transmitting messages becomes difficult, transmissions are confusing, and the probability of losing important information increases. This problem is intensified during emergencies because this condition usually generates even more radio traffic. Also, having an insufficient number of frequencies limits the use of the radio when adversaries deliberately jam the primary frequency. If too few frequencies are available, assessors should determine how the site manages the available frequencies and whether alternate communication methods are available.

When encrypted radios are in use, the procedures for installing encryption codes or for switching to the secure mode are often inadequate. Assessors should determine whether problems with encrypting codes are present and what procedures, if any, are in place for installing codes, changing data encryption keys, and switching to a secure mode. Also, radios issued to SRTs often do not have voice privacy or an encryption mode of operation.

Frequently, sites have not conducted a formal, systematic study of radio transmission and attenuation to identify dead spots and range limitations, or to determine how inclement weather affects the radio system. This is particularly important in facilities constructed with reinforced concrete. If such a study has been completed, assessors should examine the results to determine what action was taken to correct or mitigate any deficiencies.

There often are inadequate protective measures, or no protection at all, for radio antennas, repeaters, or other exterior radio components to preclude tampering and sabotage. The system control terminals and programming

stations used to monitor and administrate the system also need to be protected, and they may be located in unsecured, unalarmed locations. Further, these terminals or workstations are only provided with user-level login password protection. As the cyber threat continues to increase, these systems become even more vulnerable to a cyber attack. Two-factor authentication is one method for mitigating these concerns. Site managers' inclusion of cyber security personnel in evaluating these systems is increasingly important.

Telephones

Frequently, onsite telephone lines and switches are not protected against tampering or sabotage. Furthermore, the cellular carriers that are used for alternative communications are often not evaluated for vulnerabilities.

Duress Alarms

On occasion, hardwired alarms, switches, and junction boxes are not protected from tampering. Duress alarm equipment should be provided emergency or auxiliary power so it will continue to operate during commercial power outages.

Intercoms, Public Address, Pagers

Frequently, public address or paging systems are not provided with backup power and/or are not appropriately protected, even when they are identified as critical elements of the security communications network. As a result, these systems are often not adequate for use in contacting the majority of facility individuals during emergency conditions.

Audio Recording Systems

Frequently, recording system tapes are not kept or stored as part of the alarm station historical data. This media should be treated the same as an alarm log or record and should be stored for a pre-determined length of time.

Planning Activities

Assessors review documents and interview site personnel. Elements to cover include:

- Description of the basic communication systems, local transmitters and repeaters, and duress systems
- Types of communication equipment used in the CAS, the SAS, protective force posts, the EOC, and patrol vehicles
- Types of communication equipment issued to each SPO and SPO supervisor
- Reports documenting site performance tests of communications equipment, as well as trending reports that analyze system problems
- Operational limitations, such as dead spots and radio exclusion areas.

Performance Tests

- Radio Equipment (Appendix C, Part 1)
- Duress Alarms (Appendix C, Part 2)
- Auxiliary Power Supplies (Appendix D, Part 1).

Data Collection Activities

Assessors should tour selected areas, visually assess equipment, and verify the information gathered during interviews and document reviews. Equipment in the CAS and SAS should always be assessed. Selected fixed and mobile protective force posts should also be reviewed to ensure that equipment is operable and that personnel are familiar with communications equipment, primary and auxiliary power supplies, protection against tampering and sabotage, and operating methods.

Radio Systems

A. Assessors should review documents and interview security staff to determine whether an adequate number of radios and radio frequencies are available to the protective force, SRTs, managers, and other participants in routine and emergency conditions. If an encryption system is used, assessors should determine whether procedures are in place that adequately explain how to install encryption codes, when and how to change encryption keys, and when and how to switch to the secure operating mode.

B. By interviewing security staff, assessors can often determine whether there are transmission problems due to dead spots, inadequate range, interference, or severe weather conditions. If these problems exist, assessors should determine whether efforts have been initiated to mitigate these problems. Additionally, the analysis should include a determination of whether equipment is appropriately distributed among personnel.

C. During the assessment of entry portals, vaults, and the PIDAS, assessors should observe the effectiveness and clarity of communications. This information can assist in properly evaluating the routine use of various communication systems used by security personnel.

D. Assessors should determine whether antennas, repeaters, or other exterior radio components are protected from tampering or sabotage. Also, assessors should identify the measures used to provide reliable communications in the event of sabotage, including the primary and backup power sources.

E. Assessors should determine whether procedures are in place for testing radios and, if so, how often the tests take place and what actions are taken when deficiencies are found.

F. Assessors should examine preventive maintenance procedures to determine whether there are provisions for maintaining base, mobile, and hand-held radios and for battery replacement and charging. Assessors should also determine whether alternate methods or compensatory measures are in place when radio equipment is unavailable.

Telephones

G. Assessors should review telephones and telephone equipment to determine whether telephone lines and switches are protected from tampering or sabotage and whether operational features (for example, simplex or duplex, sound powered, or automatic ringdown) are adequate for all contingencies. This includes a review of all cellular communications as well.

H. Assessors should determine what measures are in place to provide backup communications, especially for emergency conditions, in the event that the telephone system fails.

Duress Alarms

I. Assessors should determine whether protective force posts are equipped with hardwired duress alarms and, if so, whether they are protected against tampering (for example, tamper switches, junction boxes, and line supervision). If hand-held radios do not include a duress feature, assessors should determine whether there are alternate means of indicating a duress condition. All duress alarms should be communicated without an indication at the transmitting location that the alarm has been sent. Also, assessors should identify the primary and secondary locations where duress alarms are monitored to determine whether alarm annunciation is adequate and whether protective personnel can easily identify it. Further, the auxiliary power provisions (for example, battery or generators) should be identified to determine whether they are adequate for all duress alarm systems, including radios.

J. Assessors should determine the method and frequency for testing duress alarms, including hardwired and radio. These tests can be observed at the primary monitoring station or at the individual guard posts. Also, the operator logs at the CAS and SAS can be examined to verify that tests are performed at the required frequency.

Intercoms, Public Address, Pagers

K. Assessors should review documentation and interview security staff to determine how these systems, if any, are used in communicating security information to the facility population. Elements to consider include:

- When and how pagers/cellular phones are used for security purposes
- Provisions for use in high-noise areas or electrical interference environments.

L. Assessors should verify operability by observing equipment being used or by conducting operability tests.

Audio Recording Systems

M. Assessors should interview security staff to determine whether audio recording systems record all security radio traffic, and whether duress alarms and telephone conversations are recorded. Also, assessors should determine whether recordings are stored for an appropriate period of time. Further, assessors can determine, by listening to recordings, whether radio checks and testing are performed as required, and whether radio transmissions are clear during a range of conditions. This involves listening to recordings selected from various times of the day and under different weather conditions, including periods of severe weather (such as thunderstorms). Assessors should determine whether anyone reviews the recordings on a routine basis and whether any action is taken as a result of that review. Finally, assessors should determine whether documented authorization has been obtained from the DOE Headquarters Chief Information Officer for these recordings.

Section 7: Testing and Maintenance

General Information

All PSS require the support of a comprehensive testing and maintenance program to ensure that each component remains functional and reliable. If properly conducted, testing and maintenance activities can minimize equipment failures, forecast impending operational problems, identify functional weaknesses, and guide future upgrades and improvements.

DOE orders require that security-related systems and components have a regularly applied test and maintenance program to ensure operability. If certain systems fail, compensatory measures must be implemented. Further, the people who test, maintain, or service alarm systems are required to have clearances consistent with the highest classification level being protected. Clearances are not needed if these activities are performed as bench services away from the protected location or performed under the supervision of a cleared and knowledgeable custodian, and if the systems/components are rigorously tested by cleared personnel before being placed back in service.

The following subject areas are covered in this section:

- Performance testing
  - Operability testing
  - Effectiveness testing
- Corrective maintenance
- Preventive maintenance
- Record keeping.

Performance testing is divided into two levels: operability tests that provide a simple measure of integrity on a frequent basis, and effectiveness tests that provide comprehensive assurance of integrity on an infrequent basis.

Operability testing is a continuing evaluation process that tests ACDs, IDSs, access control and screening equipment, communications equipment, auxiliary systems (power sources and lighting), and other critical systems, such as activated barriers. This testing frequency is determined by operational requirements and protection threat levels. Protective force personnel often perform operability testing.

Effectiveness testing of these systems includes more comprehensive activities that are intended to provide a high degree of assurance that they perform their intended function, even when measures are taken to attempt to avoid detection.

Details on testing personnel and procedures are provided in Appendix E. Effectiveness testing usually covers the range of performance parameters required in the facility's approved SSSP and includes the number of tests specified in the Performance Test Program Plan.

Corrective maintenance must be initiated within 24 hours of detecting a malfunction of site-determined critical system elements at facilities where Category I and II quantities of SNM, vital equipment, or Top Secret matter is protected. For critical systems, compensatory measures must be initiated immediately to provide equivalent protection to those elements that are out of service. Such measures will continue until maintenance is complete and the system element has been tested and placed back in service. These measures should be pre-determined in documented procedures.

Preventive maintenance must be performed on all safeguards and security-related subsystems and components. The frequency of such maintenance is to be documented in the SSSP or a security plan. All of the following elements are required to be included in a preventive maintenance program:

- IDSs
- CAS/SAS alarm, assessment, surveillance, automatic failover, and communication systems
- Advanced systems technologies, such as forward looking infrared, remotely operated weapons systems, and VMDs
- Communications equipment
- Personnel access control and inspection equipment
- Package and material inspection equipment
- Vehicle inspection equipment
- Security lighting
- Emergency power or auxiliary power supplies
- Keys and locks
- Protective force equipment (not including personally-issued equipment and vehicles).

The results of both operability and effectiveness tests are to be recorded and kept on file.

Common Deficiencies/Potential Concerns

An effective testing program normally includes written procedures that are intended to ensure consistency in performing testing activities, even if these activities are performed by qualified technicians who may be unfamiliar with specific equipment operation. Overall, the level of detail should be such that a competent technician can perform the required testing without significant prior knowledge of the system.

Occasionally, when the program is administered by individuals who have long tenure in performing the same activities, testing becomes routine and based on memory or experience (i.e., "skill of the craft") rather than up-to-date written procedures. In this situation, assessors should examine the program documentation to determine whether it is complete and whether it provides adequate detail to ensure continued program effectiveness if these activities must be performed by other less-experienced individuals.

Protective force personnel are sometimes improperly or inadequately trained to test the systems for which they are responsible. As a result, they perform the required tests without any in-depth knowledge of the system or comprehension of why the test is performed. For example, they may know that if they walk through a metal detector wearing all of their service equipment, the detector should generate an alarm; however, they do not realize what they have just tested. Similarly, this lack of knowledge may also apply to the many test objects used for testing the other search equipment that they routinely use.

Sometimes compensatory measures that are put in place when critical components are out of service do not provide equivalent protection. Pre-established and documented compensatory measures that address pre-identified failure modes are considered a "best practice" method of implementing this requirement.

The preventive maintenance program may not be routinely performed in a comprehensive manner to properly maintain all safeguards and security-related subsystems and components, or it may not reflect the maintenance activities that are required by the SSSP or security plan.

Records reflecting the results of both operability and effectiveness tests may not be complete.

Planning Activities

Assessors should review documents and interview security staff to determine the organizations and individuals responsible for testing, calibrating, and repairing each type of security-related system or component used by the facility. The following items should be considered:

- More than one organization may be involved with testing equipment. For example, SPOs may conduct an operability test of metal detectors, while security technicians may conduct effectiveness tests.

- More than one organization may have responsibility for a system or component. For example, SPOs may perform routine tests of SNM detectors, MC&A technicians may be responsible for calibration, and security department technicians may be responsible for repair.

Elements to cover include:

- Testing and maintenance procedures for all security-related systems

- Frequency of testing for security-related equipment, including emergency generators, security lighting, and battery backup systems

- Type of records maintained, the record-keeping responsibilities of each organization, and the locations where records are stored

- Performance of trend analyses on maintenance requests to identify aging or problematic equipment or equipment types.

Performance Tests

All performance tests cited in the appendices may be relevant to assessment of the testing and maintenance subtopic.

Data Collection Activities

Organizational Considerations

A. Assessors should identify the method of communicating requests for testing or maintenance from one department to another to determine whether the method is timely and responsive. A reasonable approach is to select several completed work requests and track their progress through the system. Assessors should ask such questions as who originated the request, how and when the request got to the maintenance department, how it was scheduled, and who verified that the work was accomplished.

B. Assessors should determine the role of vendors or outside companies in the maintenance and repair of security-related components, especially central processing units or other complex equipment. Formal procedures must be in place for tests, maintenance, calibrations, troubleshooting, and repairs. Typically, quality assurance (QA) features are in place to ensure that maintenance is performed properly and security concerns are covered, such as the two-person rule being enforced during tests or maintenance. Normally, an organization is tasked to conduct independent audits to ensure compliance with site-specific and DOE requirements. Assessors should examine these audit results to determine whether they are comprehensive and what action is taken when deficiencies are found.

C. At facilities with Category I or II SNM or vital equipment, assessors should review the DOE-approved security plans to determine the site-specific requirements for tests and maintenance. Document reviews and interviews should reveal whether these requirements are being met and, if not, the reasons for non-compliance.

D. At facilities with classified matter in LAs (or other security areas), assessors should review the DOE-approved security plans to determine whether site-specific requirements for testing and maintenance of alarm systems are followed, and whether compensatory measures are implemented (if required) when security-related subsystems or components are not in service.

E. Assessors should confirm the clearances of all maintenance staff to ensure that clearances are consistent with the highest classification level being protected.

Procedures and Operations

F. Typically, assessors should review test, maintenance, calibration, and repair procedures to determine whether:

- Procedures are clear and complete.
- They have been reviewed and approved.
- Appropriate test tools are used.
- All security-related organizations, such as protective force and security equipment technicians, have procedures specific to their duties.

G. Assessors should observe facility technicians conducting tests, maintenance, calibrations, and repairs to determine whether site personnel have and use the procedures consistent with site policies. These observations may be accomplished separately or in conjunction with performance tests.

H. Assessors should review reports developed as part of the QA program. These documents may include audits, assessments, and independent reviews. The type and extent of the QA program should be determined, and assessors should note how the facility resolves findings, issues, or deficiencies noted during QA reviews. Occasionally, the resolution process fails to adequately correct problems, resulting in a superficial treatment rather than an appropriate remedy that addresses the root cause of the issue.

I. Assessors should determine whether testing and maintenance are performed on the approved schedule. Testing or maintenance that is not performed or is performed late (e.g., equipment awaits repair for an extended period) may indicate inadequate staff or lack of management attention. Testing and maintenance should also be reviewed to determine whether security managers can direct and prioritize the activities of test and maintenance personnel (for example, whether they are dedicated to the security department or take their direction from other departments, such as facility engineering). If security technicians do not report directly to security managers, assessors should determine how the security managers control and prioritize activities – in particular, how items that need immediate attention are handled.

Training and Qualification

J. Assessors should review the training and qualifications of security technicians by reviewing resumes and records of formal training and determining whether in-house training is comprehensive.

Equipment Performance

K. Assessors should examine performance test results to evaluate equipment performance, which is the best indicator of the quality of the testing and maintenance program. If equipment performs well during performance testing, it is a good indication that the testing and maintenance program is adequate.

Records Review

L. Assessors should review records of tests, scheduled maintenance, and calibration to verify that these activities are conducted as scheduled and that records are maintained as required. Typically, assessors review records of three or four components (for example, perimeter sensors, metal detectors, and SNM detectors). If more than one organization has a major role in the testing and maintenance program, assessors should review selected records of each organization to ensure that all such records are in order. One way to facilitate the record review is to select a specific time frame and review the records of the tests and maintenance conducted during that period. The time frame selected should include six to eight test periods. For example, if a component is tested weekly, a period of two months is appropriate, and if a component is tested monthly, a period of six months may be necessary. During the record review, assessors should determine whether:

- Tests are conducted as scheduled.
- Maintenance and calibrations are conducted as scheduled.
- Records are complete.
- Documentation is legible and consistent with site-specific procedures and requirements.
- Deficiencies noted during tests or maintenance are promptly reported and appropriate action is initiated (that is, compensatory measures or work orders). Often, assessors can verify that maintenance action was initiated by listing deficiencies and dates noted on test records, then checking maintenance logs or work order requests to verify that action was taken and to determine time frames for corrective actions. Assessors can also verify that compensatory measures were initiated as required by checking the protective force supervisor's or CAS operator's logs.

M. Assessors should review records of equipment repair, replacement, and corrective maintenance. One way of conducting this review is to select a sample of repair records and trace the documentation back to the initial report of failure (or vice versa). This process typically involves reviewing records of:

- Equipment failures reported by SPOs or other organizations

- Tests that indicate deficiencies requiring maintenance

- Communication of either of the above items to a supervisor or other person who develops a maintenance request

- Assignment of maintenance responsibility (work order) and date that work was initiated

- Date and time that work was completed and names of personnel accomplishing task

- Verification that the work was completed and closeout tests were conducted.

With this process, assessors can determine:

- Whether records are complete.
- Time frames for initiating and completing repair.

- Whether documentation is complete.
- Whether site-specific policies and procedures are followed. (For example, if a two-person rule is in effect, were two qualified individuals assigned to the task?)

Section 8: Support Systems

General Information

PSS support systems include power supplies and tamper protection associated with intrusion detection equipment, alarm monitoring and assessment systems, access control, and entry/exit screening equipment. This section also addresses the application of regulatory warning signs.

For the purposes of security systems, auxiliary power is defined as a backup power system (battery and/or engine-driven system) that provides emergency electrical power to security systems when normal power is lost. In the event that the primary power source fails, DOE requires that transfer to auxiliary power must be automatic without affecting the security system or device being protected. Both the CAS and the SAS must receive an alarm indicating failure of any power source and transfer to auxiliary power. Auxiliary power supply configurations vary widely throughout the DOE complex, depending upon the system, the equipment, and the manufacturer. The need for auxiliary power, based on the safeguards and security interests being protected, should be documented in the site security plan.

Assessors should evaluate auxiliary power supplies to determine whether they are adequate to power all alarm systems and critical equipment long enough to permit restoration of normal power, or until other compensatory measures are implemented.

Use of batteries is one method to provide auxiliary power, and a number of provisions are related to their use. When rechargeable batteries are used, they should be kept fully charged or subject to automatic recharging whenever the voltage drops to a specified level. Non-rechargeable batteries should be replaced when their voltage drops 20 percent below the rated voltage. An alarm signal should be activated to indicate this condition.

Various methods are used for detecting and preventing attempts to tamper with security systems. Tamper protection is addressed more fully in Appendix D, where tests are identified that verify proper operation of tamper detection components. If operational or process control information, such as low sample rates, incorrect pressure readings, or unusual airborne radiation levels, is relied on for security purposes, then these systems should also be checked for tamper resistance.

Tamper and line supervision tests are usually conducted in conjunction with related tests of CCTV equipment and the intrusion detection and access control systems to verify the effectiveness of the tamper indicating equipment.

The posting of signs listing regulations and penalties is addressed by the Atomic Energy Act of 1954. Typically, these signs list prohibited activities, such as unauthorized entry onto DOE property, and the associated fines or imprisonment that violators may receive if convicted of these activities. Signs are normally posted at entrances and at intervals along the perimeter of the property and/or security areas. Signs posted at entrances normally list prohibited and controlled articles, such as firearms, explosives, privately owned recording and electronic equipment, cellular telephones, computers, and controlled substances.

Common Deficiencies/Potential Concerns

Often, supporting devices associated with auxiliary power sources are not afforded adequate tamper protection. These may include:

- Batteries
- Inverters
- Power switches
- Fuel supplies.

When one or more of these items are disabled, the auxiliary power source may be effectively neutralized. For example, a fuel tank may furnish fuel to a generator that is the primary backup power source for a particular security system. If the fuel tank is contaminated or destroyed, the backup power source is effectively eliminated, even though the generator itself may be adequately protected.

Since batteries can be hazardous (battery acid can burn or be extremely corrosive), routine servicing and testing are important. Sometimes, assessors find batteries left unattended and in poor condition. Some associated problems can be identified early in the assessment by checking testing and maintenance procedures.

The most significant concern in the area of tamper protection is the frequent failure by DOE facilities to provide complete tamper indication and line supervision for all security system elements and devices requiring protection. Tamper devices may include magnetic switches, plungers, and closure contacts. These devices should be inaccessible to an adversary and located inside a protected space or otherwise secured.

Frequently, line supervision fails to include the entire circuit to be protected (that is, the sensor itself, local wiring to a control device, the transmission medium, and the final signal processing annunciation equipment). In this case, the destruction or failure of the unprotected component could result in the failure of the whole system.

In some cases, multiple tamper devices are included on a single alarm circuit to reduce wiring and signal processing requirements. This can be a significant weakness since the actual type and location of the alarm, and the number of affected devices, may not be apparent from the information displayed at the alarm console.

Planning Activities

Assessors review documentation and interview facility representatives to gather information on auxiliary systems, including power supplies and tamper alarms. If vital or security-related equipment relies on cooling water (for example, reactor coolant pumps) or fuel supplies (for example, engine-generator sets), assessors should determine what methods the facility uses to ensure the reliability of such systems.

Performance Tests

All performance tests cited in the appendices may be relevant to assessment of support systems, especially those pertaining to auxiliary power supplies and tamper alarms (Appendix D).

Data Collection Activities

Power Supplies

A. Assessors should interview security staff and review documents to determine:

- What security-related components are supplied auxiliary power by batteries, a UPS, or other means
- How long the UPS can maintain operation at full load, and procedures for load shedding
- Number and location of engine-generator sets (normally diesel generators)
- Security-related components that are supplied auxiliary power by engine-generator sets
- How long engine-generator sets can maintain load until the fuel supply is exhausted

- Frequency and methods of testing and maintaining engine-generator sets (for example, full load tests, test of switching devices)

- Frequency and methods of testing and maintaining system batteries or the UPS

- Frequency and methods of testing and maintaining batteries that power individual components (for example, sensors)

- Replacement frequency for non-rechargeable batteries

- Indications received in CAS/SAS when normal or auxiliary power fails

- Source of offsite electric power, including number of feeds

- How the systems are tested (are they turned on, brought up to speed, and load-switched, or does the test actually simulate power loss?).

B. Assessors should tour areas where components critical to providing auxiliary power are located and verify the information gathered during document reviews and interviews. Items of interest include fuel supply reservoirs, switching equipment, batteries, and power-generating equipment. All of these elements should be given adequate physical protection, including tamper protection and shielding from inclement weather. For example, the switching equipment for the commercial-to-auxiliary power transfer should not be installed on the outside of a security area where access is unrestricted and tampering could go undetected.

Tamper Protection

C. Assessors should review the methods in place to prevent and detect attempts to tamper with security-related systems, including the use and assessment frequency of tamper-resistant hardware and tamper-indicating devices (TIDs). Also, assessors should review the general installation techniques for security sensors (that is, the use of epoxy over screws or bolts, security seals, or deformation of threads on attachment hardware). If operational or process information is used for security purposes, this equipment should have many of the same physical protection features as security equipment. The use of TIDs and security hardware should also be reviewed, including the level of confidence or response placed on this type of alarm (that is, does the protective force initiate a full-blown response or is an SPO dispatched to investigate the alarm?).

Signs

D. Assessors should determine whether the required signs are appropriately placed and in good repair as required by the DOE orders and site security plans. Signs should include, at a minimum:

- Atomic Energy Commission
- Prohibited articles
- LA
- Vehicle and personal searches
- Surveillance in use.

Section 9: Systems Management

General Information

Systems management is an important component of the PSS topic and merits specific attention to verify that security management personnel provide sufficient planning, direction, and control processes to ensure continued effective performance of all PSS components.

Management personnel have the responsibility to ensure that security interests are adequately protected and that the levels of protection for each of those interests are provided in a graded fashion in accordance with potential risks. In order to meet this responsibility, they perform a number of activities, including:

- Developing plans that include goals, objectives, and responsibilities for every aspect of physical protection
- Preparing and implementing procedures and policies that consider site-specific conditions and fulfill DOE requirements
- Providing adequate resources – including personnel (plus training), equipment, and facilities – to meet the requirements contained in the procedures and policies described above
- Defining organizational and individual responsibilities (including accountability for performance)
- Performing management oversight activities, such as self-assessments and surveys, to identify areas of security weakness that need to be strengthened
- Monitoring the status of programs and policy implementation
- Correcting all areas of weakness in a timely and efficient manner.

Common Deficiencies/Potential Concerns

The following subtopical areas are specifically noted where weaknesses are sometimes found to negatively impact the effectiveness of the overall PSS program. This list represents common areas of concern, although there may be other weaknesses in these and other areas.

Management Responsibility for Safeguards and Security

Management Support and Oversight. DOE and facility operations and production managers sometimes prioritize production or operational goals above security goals and are reluctant to commit limited/competing resources to address security needs or to implement physical security measures that may be inconvenient to site personnel or that may impact production activities. In these cases, senior management must strike an appropriate balance between security, site operations, and production goals. Management personnel in the security organization, along with other senior managers, must ensure that all necessary measures are maintained to adequately protect the site's security assets.

Organizational Structure. In some instances, the individuals responsible for establishing and ensuring compliance with security policy and procedures are not appropriately positioned in the site organizational structure to ensure that management is fully aware of PSS needs that must be addressed. In other instances, the security organization may have little control or influence over engineering and/or maintenance personnel who are responsible for design and/or ongoing maintenance of certain PSS components. In all of these instances, senior management must be properly informed to ensure that security needs are appropriately addressed.

Responsibilities. Responsibility for all aspects of PSS installation, operation, maintenance, and testing may not be specifically assigned and properly documented. Inadequate assignment of responsibility inevitably results in some PSS functions not being properly performed.

Staffing. Insufficient staffing levels may occur when an adequate number of people are available but they lack sufficient skills and training to perform specific tasks. Other areas of staffing concern could result from supervision that is inadequately trained or assigned excessive additional duties.

Personnel Competence and Training

Training. In certain instances, inadequate training can be the root cause of PSS-related deficiencies. The level and quality of PSS-related training vary widely among DOE facilities. In some instances, a significant component of PSS maintenance training activities consists of trainees obtaining specific, detailed information from other more senior personnel using skill-of-the-craft techniques. This training method is sometimes implemented without measuring the effectiveness of the training or the acquired competence of the trainee. Regardless of training techniques, the adequacy of PSS performance is a measure of their effectiveness.

Comprehensive Requirements

Planning. PSS planning activities related to risk associated with security assets are generally conducted by security specialists who evaluate site-specific risk resulting from pre-defined and locally identified threat scenarios. In some instances during these planning activities, some potential threats, adversary approaches, and/or insider scenarios that may initially be regarded as unconventional or unrealistic are not fully considered. As a result, security concerns that would otherwise be identified may not be adequately addressed in the appropriate planning documents, such as the SSSP and supporting VAs for Category I SNM facilities. Failing to consider the full spectrum of potential security concerns may hinder PSS normal functionality.

Implementation of Requirements. DOE facilities develop policies and procedures that guide and direct the protection of identified security interests. However, if those policies and procedures are not properly implemented, they will provide less than the intended protection levels.

Feedback and Improvement

Self-Assessment Process. Not all facilities have fully implemented a comprehensive self-assessment program in order to provide security management a continuing overview of performance related to various components of their security program. In these instances, deficiencies could go undetected and uncorrected for extended periods.

Corrective Action Plans. Corrective action plans are developed to identify steps that are needed to resolve identified deficiencies. Incomplete or improperly developed plans may result in deficiencies not being corrected. To prevent the recurrence or occurrence of identified risks, the systematic investigation of the root causes of failure should include the following steps:

- Identify root causes/issues associated with the deficiency, and ensure that the identified items are not just symptoms.

- Develop corrective action plans to mitigate the deficiencies by addressing the root cause issues.

- Prioritize deficiencies to correct the most serious ones first, rather than correcting those most recently identified.

- Establish a corrective action schedule with milestones so progress can be monitored and schedule slippages identified early.

- Assign responsibility for completion to specific organizations and individuals.

- Continually update the plan if new milestones are needed to resolve the deficiency.

- Ensure that adequate resources are applied to correcting deficiencies in a timely manner.

Planning Activities

Assessors should interview facility personnel during planning activities and review available documentation (for example, SSSP, procedures, self-assessments, survey reports, and other pertinent documents) to characterize the program. Assessors should:

- Determine the organizational structure, including whether a central group establishes and monitors compliance with procedures. If not, determine how many separate points of authority for the program exist among the various organizational elements.

- Review organizational charts and identify the names of all persons with PSS supervisory and managerial responsibility.

- Determine how PSS policy and procedures are promulgated and distributed.

- Determine how the self-assessment program functions, including:

  - Frequency of self-assessments
  - Who has overall authority for the program
  - Who actually performs the self-assessments.

- Focus on determining whether the self-assessment program provides an independent evaluation of PSS or whether it is conducted by the same persons who operate the programs being assessed.

Once assessors understand the structure of the program, they should determine which organizations and program elements will be reviewed in more depth during the assessment and which individuals will be interviewed. At large facilities, it is not practical to assess all systems in the same depth or to interview all individuals who perform systems-related duties. In such cases, a representative sample may be selected for evaluation. For reasons of efficiency, the review of systems management is normally performed by assessors who are also assessing other PSS subtopics. Consequently, the assessment team should consider a variety of factors when selecting organizations to review. It is usually advisable to interview first-line managers with responsibility for the systems that are selected for performance tests; this ensures that the impact of any deficiencies identified during the reviews can be covered with managers during the management interviews. In addition, the information gathered during the first few days of the assessment often influences the selection of managers to be interviewed. As program strengths and weaknesses are noted, the assessors should modify their planned activities appropriately.

Assessors review basic documentation and interview facility security and protective force representatives to determine how security-related procedures are implemented. Areas to review include:

- Post orders
- Repository checks

- Alarm responses
- SNM transfers
- Emergency response
- Training.

Such reviews should be closely coordinated with the other topic teams to maximize efficiency. The PSS team focuses on the protective force interface with security systems and does not evaluate the tactical capabilities of the protective force (for example, weapons-related skills or the ability to use cover and concealment).

Assessment Process

Assessors engage in numerous activities during the assessment process to evaluate the performance effectiveness and compliance with requirements for PSS and the associated subsystems and components. The remainder of this section is devoted to describing various steps and activities that assessors may find useful in evaluating management activities associated with operation and maintenance of PSS. The usefulness of these items will vary widely, depending on the conditions identified at each specific site. Furthermore, those site-specific conditions may dictate that different steps and activities may be more appropriate.

Data Collection Activities

Line Management Responsibility for Safeguards and Security

A. Assessors should review the applicable planning documents that cover PSS (for example, SSSPs or other planning documents). Particular attention should be devoted to determining:

- Whether the planning documents are current
- Whether they appropriately identify:
  - Goals
  - Objectives
  - Responsibilities
  - Overall policies for all aspects of PSS
- Whether they address all applicable security interests.

B. Assessors should identify any special conditions or unique features of the site that are covered by exceptions or alternative approaches to determine whether the facility has documented the justification for the exceptions.

C. Assessors should interview security managers, including design and testing/maintenance supervisors, and review resource plans and budget documents. Elements to cover include:

- Whether goals and objectives are clearly defined
- Whether needs identified in the corrective action plan and strategic plan (if one exists) are reflected in budget documents
- How well the PSS budgeting process functions
- Whether staffing plans are consistent with budget requests.

D. Assessors should determine whether the organizational structure facilitates efficient communication and positive working relationships between the various organizational elements, and between persons who deal with PSS. The functional relationships between the various organizational elements should be clearly defined, formally documented, communicated, and understood by all persons. One method useful for investigating the adequacy of the communications and interactions between organizational elements is to determine how the organizations interact with one another (for example, protective force and MC&A) when facility conditions change (for example, during material transfers between security areas).

E. Assessors should determine whether individuals responsible for ensuring that PSS components perform effectively are in a position within the organization to ensure that identified weaknesses are adequately addressed. This may involve reviewing the facility's policies and procedures to determine whether those individuals have the authority to resolve issues identified during self-assessments and other similar activities.

F. Assessors should interview managers in the security department and operations and production departments to determine whether the security organization has any problems getting operations or production personnel to implement required procedures. If initial interviews indicate questions about the operations or production organization's commitment to implementing required security measures, assessors may elect to conduct more detailed interviews (e.g., with higher-level management) and document reviews to determine whether problems exist. This detailed review may involve examining findings identified in self-assessments, surveys, and assessments to determine whether corrective actions were implemented in a timely manner, or whether repeated memoranda from the security organization are necessary before operations or production personnel take action. Other indicators of problems include a pattern of repeated deficiencies at the same location.

G. Assessors should determine how management communicates its goals and objectives and stresses the importance of PSS. Assessors should determine what incentives are used to encourage good performance.

Personnel Competence and Training

H. Assessors may elect to review a sample of position descriptions for specific individuals who have responsibilities for PSS to verify that responsibilities are actually reflected at the individual's level. Assessors can also review individual position descriptions and performance goals of technicians or other persons in the operations and production departments who conduct performance tests or perform maintenance functions to determine whether they are held accountable for their performance and whether good performance in PSS-related areas is specified in these documents.

I. Assessors should compare actual and authorized staffing levels for PSS positions to determine whether the program is operating short-handed. Assessors must be especially watchful for non-PSS responsibilities being assigned to key program personnel, detracting from their ability to perform their PSS duties.

J. Assessors should review training plans, course materials, and training needs analyses and conduct interviews with security staff, operations/production supervisors, and custodians. Assessors should observe training classes for personnel who address any aspect of security-related functions, such as:

- SPOs
- PSS technicians
- PSS testers
- Custodians
- Operators
- Health physics staff.

Training reviews indicate whether operations and field personnel understand the security concerns underlying their operations (not only the security practice, but the reason for the practice). For example, the SPO responsible for monitoring a metal detector may have been given orders that all incoming personnel must clear the metal detector, but no orders regarding outgoing personnel. If the SPO does not fully understand the purpose of the metal detector (to prohibit the introduction of weapons and contraband and to prevent removal of SNM or DOE property), the SPO may fail to ensure that outgoing personnel clear the metal detector.

K. Assessors should review training records and test scores and interview personnel who have received training to verify that training has been conducted as scheduled and that personnel have attended courses as required. During interviews, assessors should ask facility personnel questions taken from facility tests as a means of determining the effectiveness of the training program. Assessors may also ask personnel to perform the functions for which they have been trained (for example, test an alarm sensor, apply a TID, operate a hand-held SNM detector). In this manner, assessors can observe each individual's knowledge and skills and verify the training program's effectiveness.

Comprehensive Requirements

L. Planning – Airborne Protection. Assessors should review the SSSP to determine whether airborne assault is to be considered as a site-specific threat. If so, the assessment team should evaluate all airborne denial barriers and detection equipment. In those cases, assessors should review documents and interview security staff to determine the level of protection against airborne intruders. Items to check include whether:

- Helicopter barriers (for example, poles and rope systems) have been installed to protect priority targets.

- An electronic detection system is used (for example, acoustic detectors or radar). If so, the methods for testing effectiveness should be reviewed.

- Other means of detecting airborne intrusion are available (for example, patrols, or SPOs in exterior posts).

Assessors should also tour areas to determine the degree of protection against airborne threats. Items to note include:

- Potential landing sites that could be used by helicopters, gliders, parachutists, or fixed-wing aircraft
- Factors affecting the likelihood of detecting airborne intrusion, such as:

  - The size of the area
  - Visual detection capability from guard posts
  - Frequency of patrols
  - General level of activity in the area

- Effectiveness of any aircraft denial barriers, including susceptibility to defeat by covert means.

M. Planning – Insider Analysis. Assessors should evaluate the vulnerability of high-security facilities (for example, those with Category I SNM or vital equipment) to possible compromise by insiders, including:

- SPOs
- CAS and SAS operators
- Custodians
- Operators
- Supervisors

- Security technicians
- Maintenance personnel
- Health physics technicians
- Emergency response personnel (for example, firefighters)
- Armorers
- Locksmiths.

Vulnerability to insiders can be evaluated by reviewing VAs, interviewing personnel in various job categories, and systematically examining the job duties, responsibilities, and "privileges" of personnel in selected job categories (for example, possession of master keys, access to safe combinations, capability to place alarm systems in access mode). Assessors should pay particular attention to personnel who have access to SNM and who have numerous responsibilities (for example, material custodians who also test alarms, have safe combinations, and enter information into accountability systems). Assessors should also look for possible single-point failures (for example, areas where the entire safeguards system would be ineffective if one element were to fail) and determine whether the elements possibly involved in such failures are vulnerable to insider sabotage.

N. Requirements Implementation – Material Surveillance Procedures. Assessors should conduct the following activities:

- Review such documents as the MC&A plan, operating procedures, and the SSSP.
- Interview security staff, material custodians, operators, and other personnel who use or process SNM.
- Tour process areas to determine what methods are used to provide surveillance of material that is not in secure storage.

Material surveillance of SNM must be maintained within use and process areas. A two-person rule is a common method of implementing material surveillance at Category I or II areas. Custodial and administrative controls are generally used in Category III or IV areas.

The assessment team should pay particular attention to the means of providing material surveillance for SNM that is kept in process storage or staging areas. Assessors should ensure that all practices are consistent with MC&A plan provisions and effectively implemented.

The effectiveness of the two-person rule should be evaluated by reviewing and observing procedures. Assessors should verify that procedures are developed for all areas and distributed to all personnel who must implement them. The procedures should clearly specify what is required (for example, constant visual contact, two persons in the same room, or two persons in the same vault). The means of enforcement of a two-person rule at MAAs or vault entrances can also be reviewed. Card-reader systems, SPO procedures, and double-lock systems are common methods for enforcing a two-person rule. In some areas, assessors may also review access logs to determine whether the two-person rule is implemented as required. Assessors should attempt to observe implementation of the two-person rule and interview material handlers or custodians to determine whether they understand and implement the requirements correctly. The PSS team's evaluation of the aforementioned activities should be closely coordinated with the MC&A team, as discussed in Section 10.

O. Requirements Implementation – SNM Transfer Procedures. Assessors should identify:

- The SNM transfer paths, including offsite shipping and receiving and intra-site transfers, and the category and classification of SNM transfers

- Specific portals used for SNM transfers and the controls implemented at those portals by the operations, production, and health physics staffs, and by the material custodians and the protective force

- Escort procedures, including the number of armed SPOs who accompany Category I shipments
- Vehicles used for shipments, including special security features of vehicles (for example, remote-disable capability, hardened vehicle, locked storage, delay features)
- Methods implemented to ensure that SNM is not diverted in non-SNM transfers and/or radioactive waste shipments.

Assessors should observe SNM transfers to determine protection effectiveness and verify the information collected during interviews and document reviews. Procedures at the shipping portal and/or receiving portal should be observed, as well as the transfer route.

Once the assessors have an operational understanding of the transfer procedures, they should evaluate them for vulnerabilities or weaknesses. One method is the "what if" approach: for example, What if the vehicle driver is the insider? Are there procedures that will prevent the driver from driving away with the material?

P. Requirements Implementation – Emergency Procedures. Assessors should conduct the following activities:

- Review documents, such as SSSPs, standard operating procedures, emergency plans, post orders, and other documents.
- Interview security managers, protective force supervisors, custodians, and operations/production supervisors.
- Tour use and process areas to identify the methods used to ensure the security of SNM during and following emergency alarm activations (the evaluation should include response to other security alarms that may occur during one of these emergency events):
  - Evacuation alarms
  - Fire alarms
  - Criticality alarms
  - Medical emergencies
  - Radiation alarms
  - Toxic chemical situations.
- Review requirements and conditions for post-evacuation SNM inventories.
- Identify the methods used to control evacuation, including:
  - SPO response
  - Pre-planned evacuation routes with barriers
  - Post-evacuation personnel accounting
  - Post-evacuation patrols and searches.
- Review relevant procedures, such as protective force procedures (including response plans), custodial procedures, operations/production procedures, and health physics procedures.

Assessors should verify information about emergency evacuations by observing facility tests or reviewing results of after-action reports (incident reports). For example, if evacuations have occurred, assessors can

usually review incident reports and verify that an inventory was performed as required by site-specific procedures.

Feedback and Improvement

Q. Most organizations have some type of central, integrated system to identify and follow the status of deficiencies identified during self-assessments, site office surveys, and assessments. Assessors should determine what system or systems are being used. Some sites have a comprehensive system that includes all safeguards and security-related deficiencies, while at others, each area, including physical security, has a separate tracking system. Self-assessment programs are the key to effective management oversight.

R. Assessors should review the self-assessment program in detail to determine whether self-assessments are performed regularly and whether they review all aspects of the physical security program. Selected self-assessment reports should be reviewed to determine whether root causes are identified when deficiencies are found. It is helpful to compare the results of facility self-assessments to assessment findings or other audit results to learn whether the self-assessments are equally effective.

S. Assessors should determine who actually performs self-assessments. If the persons who actually perform physical security functions conduct the self-assessments, there should be some form of independent verification or evaluation of the results. Assessors should determine whether deficiencies identified during self-assessments are entered into a tracking system, and how corrective actions are selected and carried out.

T. Assessors should determine whether an organization has a tracking system and how it operates. Assessors should determine whether there is a formal system for independently verifying that corrective actions have been completed and that the original problem has been resolved effectively. Assessors may choose to select a sample of physical security deficiencies from several sources and determine whether they were entered into the tracking system. Finally, a sample of prior deficiencies whose corrective action plans have been closed may be selected to verify that the deficiencies have in fact been adequately corrected.

U. Assessors should determine whether corrective action plans are developed, whether deficiencies are analyzed and prioritized, whether schedules and milestones are established, and whether specific responsibilities to ensure completion are assigned down to the individual level. Assessors should also determine whether root cause analyses are performed. If so, the assessors should request documentation on root cause analyses for significant deficiencies listed in the tracking system and the rationale for the particular course of corrective actions chosen. As a related activity, assessors may elect to review how the resources needed for corrective actions are introduced into the budget process.

V. Assessors should evaluate the role of DOE oversight of PSS by interviewing selected DOE security or oversight managers to determine how they perform their oversight responsibilities. Specific items to review include how contractor physical security program functions are evaluated during surveys, how DOE tracks program status, and how oversight personnel and facility personnel interact daily. Additionally, selected contractor management personnel should be interviewed on the same subjects.

Section 10: Interfaces

Introduction

Integration is the coordination and cooperation among assessment team members designed to achieve a more effective and organized assessment effort. It creates a synergism that results in an enhanced knowledge of the assessed site, a strengthening of assessment techniques, and a more comprehensive assessment report. The integration effort significantly contributes to the effectiveness of the EA assessment process and, along with other unique attributes, enhances its ability to provide an accurate, in-depth evaluation of protection programs throughout the DOE complex.

Because of the interdependency of elements of any security system, integration must continue throughout all phases of the assessment to ensure that all pertinent data has been shared. Integration, facilitated by nightly team meetings, is realized by exchanging information and discussing how information collected by one topic team influences the performance of security system elements observed by other topic teams. The fundamental goal of this effort is to ensure that potential systemic vulnerabilities are clearly identified and analyzed.

In addition to enhancing assessment results, integration has several other major benefits. First, it allows topic teams to align their efforts so that their activities complement rather than detract from one another. It is usually less productive to assess PSS at one location, classified matter protection and control at a different location, and the protective force at yet another location. Using this approach, assessors would accumulate a collection of unrelated facts. Therefore, topic teams must cooperate to make the best choices regarding what should be assessed at which locations. Early and continuing integration helps ensure that the activities of all topic teams are unified and contribute to the overall goal.

A second benefit of integration is that it allows topic teams to benefit from the knowledge, experience, and efforts of other topic teams. Sometimes, ideas developed by one topic team can help another topic team focus assessment activities in a more productive and meaningful direction. For example, the PSS topic team may indicate that its planning effort led to the conclusion that the physical protection systems at a particular location are weak, resulting in heavy reliance on the protective force. It may therefore be useful for the protective force topic team to plan to focus on assessing protective force capabilities as they relate to this weakness, in addition to their independently determined areas.

The third benefit of integration is to prevent topic teams from interfering with each other. Often, several topic teams concentrate their activities at the same location, resulting in multiple visits over time or a number of visits at the same time. This causes undue disruption of the facility being assessed. Integration among topic teams can preclude this problem by having one or two topic teams visit a particular location and collect the data for several. All topic teams should be aware of what all other topic teams are doing, where they are doing it, and how it will affect their own activities.

Integration of data collection activities for performance testing is imperative. For example, if the PSS topic team schedules a performance test that results in the activation of the alarm system in a building, and the MC&A topic team simultaneously schedules a performance test involving an emergency inventory or transfer of material in the same building, the result may be that neither team can collect the necessary data.

As an integral part of the overall protection program at any DOE facility, PSS interacts with all other elements of that program. Therefore, the topic cannot be assessed in isolation. Assessment team members must continually keep this in mind in order to determine how well this interaction works. As noted, this requires integration with topic teams responsible for other assessment areas. Information developed by these teams may affect how the results of the PSS team efforts are viewed. Similarly, data gathered by the PSS team may have some bearing on how the results of another team's efforts are viewed.

Protection Program Management

The PSS topic team must consider elements of protection program management, because they are mutually supportive. Evaluating the consistency of descriptions contained in the SSSP with the actual system or procedural configurations involves mutual validation between the protection program management and PSS topic teams. Another area of mutual support is the implementation of the DOE ISSM program at a facility and how it supports PSS, maintenance, personnel, and management's attention to the resources needed for a successful program.

Classified Matter Protection and Control

This topic relates to PSS because requirements for protecting classified information and material include:

- Control and storage of documents
- Physical control of classified components
- Establishment of security areas for classified information processing, including secure communications centers
- Alarm log printouts, alarm system drawings, and compensatory plans
- Protective force patrols (also reviewed by the protective force team)
- Badge and pass systems.

Personnel Security

The PSS topic team must consider elements of personnel security when the site places high reliance on the adequacy of its personnel security programs. Implementation of human reliability or personnel security assurance programs may directly affect the overall PSS program. Also, PSS may interface with personnel security in the areas of visitor control and escort procedures. Personnel security systems that interface with PSS should be afforded the same level of protection as the systems they interface with.

Material Control and Accountability

The interface between the assessment of PSS and MC&A is important to ensure that findings are reported in the appropriate topic and that both assessment teams are aware of potential problem areas impacting their individual conclusions.

DOE orders require MC&A procedures to be compatible with the physical protection and security of the system.

The PSS and MC&A topics overlap in a number of areas, including:

- Surveillance of SNM
- Access controls and records
- MAAs
- Portal monitors
- Material transfers
- Storage of materials
- Detection of unauthorized activity or conditions.

If both topics are assessed at the same facility, any findings involving areas of overlap should be coordinated between the MC&A and PSS topic teams to ensure that findings are reported under the most appropriate topic. Typical findings of mutual interest include:

- Access controls that do not meet DOE requirements
- Deficiencies in barriers that could allow an insider to divert material out of a security area without detection
- Deficiencies in the IDS protecting SNM storage repositories or security area perimeters
- Deficiencies in locks, key control, or combination controls that could allow an insider to gain unauthorized access to SNM
- Portal monitor capabilities that are ineffective or inconsistent with the type of material in the MAA
- Inadequate implementation of procedures, such as the two-person rule or vault closing/operating procedures
- Category I quantities of SNM stored outside a vault or vault-type room.

The interface with the MC&A topic team frequently results in identifying locations of special concern because of the category or attractiveness of material in process or storage. This information can significantly redirect the focus of the PSS assessment. For example, if a significant quantity of SNM is identified as being outside the MAA during assessment planning, it may initially be considered a major problem. However, subsequent coordination between the MC&A and PSS teams may reveal that there is no problem because of the condition of the material and the storage method. In this case, both teams can refocus their attention and assessment activities.

Protective Force

Interface with the protective force topic team is very important in performance testing. In addition, the subtopic of badges, passes, and credentials is of interest to a variety of EA assessment teams (typically personnel security, classified matter protection and control, and protective force). Although the PSS team reviews the badge system, the personnel security, protective force, and classified matter protection and control topic teams must be kept informed of results, because they may also review some aspects of the badge system. For example, the personnel security team may review the procedures for issuing badges, and the protective force topic team often observes badge-checking procedures at portals. Performance tests conducted by protective force assessors also have a bearing on any conclusion drawn by PSS assessors. Consequently, all of these topic teams must coordinate their efforts both to ensure full coverage and to avoid duplication of effort.

The PSS team can increase the efficiency of its data collection efforts by having the protective force team help collect data at the portals. For example, PSS assessors may provide the protective force assessors with a short list of information to gather at each post as part of the post checks. Examples of information that might be more efficiently collected by the protective force team include whether SPOs are knowledgeable about policies for accepting badges of other contractors, whether each post has a current list of lost badges, and whether the post orders are consistent with site policies.

Cyber Security

Cyber security assessments are conducted by the DOE Office of Cyber Assessments, often in conjunction with a PSS review, and they routinely involve an evaluation of the effectiveness of the security controls implemented on computer systems used to operate automated access control and IDSs, along with badging and video monitoring systems. This interface is especially important because data processed by these computers at many facilities is not classified, so the computer systems are not subject to the same strict security requirements as classified systems. Because of the diversity of security alarm system applications, the PSS team must work closely with the cyber security team to identify potential vulnerabilities associated with security-related computer networks.

Section 11: Analyzing Data and Interpreting Results

Introduction

This section provides guidelines to help assessors analyze data and interpret the results of data collection. The guidelines include information on the analysis process, including factors to consider while conducting an analysis. Information is also included on the significance of potential deficiencies, as well as suggestions for additional activities when deficiencies are identified. After completing each activity, assessors can refer to this section for assistance in analyzing data and interpreting results and for determining whether additional activities are needed to gather the information necessary to accurately evaluate the system.

When analyzing the data collected on a particular aspect of the site security system, it is important to consider both the individual segments of the security system and the system as a whole. In other words, failure of a single segment of a security system does not necessarily mean the entire security system failed. This is one reason why integration among topic teams is so important. It provides for a look at the "big picture" within the framework of the site mission when determining whether the overall security system is effective.

Assessors must be aware of the relationships between the various elements of a particular PSS and between one PSS and another. For example, a barrier system might form the first layer of protection for more than a single asset. In one case it may be the only layer of protection, and in another it may be one of several layers. Auxiliary power systems may support several elements within a PSS. Recognizing these dual roles precludes duplicative testing efforts and places the particular element in proper perspective.

All elements of a properly designed PSS interface with one another and are interdependent. Entry control, intrusion detection, and barrier systems are directly related. Testing and maintenance is interwoven throughout all system elements. Auxiliary systems, such as power-generator sets, play a supportive role in the functioning of the overall PSS.

Analysis of Results

The information collected for each of the PSS subtopics is reviewed to determine whether the PSS complies with the requirements of DOE orders. In addition to compliance, the analysis process involves topic team members' critical consideration of all assessment results, particularly the identified strengths and weaknesses or deficiencies, framed within the parameters of the site mission. Analysis should lead to a logical, supportable conclusion regarding how well PSS are meeting the required standards and satisfying the intent of DOE requirements.

A workable approach is to first analyze each subtopic individually. The results can then be integrated to determine the effects of the subtopics on each other and, finally, the overall status of the topic. As mentioned before, it is important to weigh the significance of a weakness or deficiency in light of the entire system. For example, if one intrusion detection device is inoperable, is the entire IDS deficient? What other measures or backup devices compensate for the deficiency? If barriers, other alarm systems, and CCTV cameras are in place, do they ensure that protection needs are being met?

If there are no deficiencies, the analysis is relatively simple. In this case, the analysis is a summary of the salient assessment results supporting the conclusion that protection needs are being met. If compensatory systems or measures were considered in arriving at the conclusion, these should be discussed in sufficient detail to clearly establish why they counterbalance any identified deficiencies.

If there are negative findings, weaknesses, deficiencies, or standards that are not fully met, the analysis must consider the significance and impact of these factors. The deficiencies must be analyzed both individually and

collectively, then balanced against any strengths or mitigating factors to determine their overall impact on the PSS's ability to meet DOE requirements and site mission objectives. Deficiencies identified in other topic areas should be reviewed to determine whether they have an impact on the analysis. Other considerations include:

- Whether the deficiency is isolated or systemic
- Whether the site office or contractor management previously knew of the deficiency and, if so, what action was taken
- Mitigating factors, such as the effectiveness of other protection elements that could compensate for the deficiency
- The deficiency's actual or potential effect on mission performance or accomplishment.

Interpreting Results

PSS must provide the desired level of protection for the asset(s) for which they are deployed. It is not enough that the various individual component parts of a system or systems meet manufacturers' specifications.

The SSSP and supporting documents can provide a link from DOE-wide performance expectations, including the DOE generic threat, orders, and policies, to facility-specific performance expectations.

Exterior Intrusion Detection and Assessment

When the perimeter can be frequently crossed without detection in one or more zones, the perimeter sensors likely are unreliable. This weakness must be analyzed in light of site-specific protection objectives and complementary systems. On the other hand, when one or more sensors can be defeated but redundancy in the sensor configuration is successful in detecting an intruder, the deficiencies are of lesser concern because the combination of sensors is effective. However, this problem may indicate testing and maintenance deficiencies.

When the facility indicates that a system is correctly calibrated but tests indicate that the sensors are not reliable, that condition may be the result of an isolated instance of sensor drift or of deficiencies in the facility's testing and calibration procedures. A large number of sensor deficiencies may indicate problems with the testing and maintenance program or the QA program. In this event, assessors may consider testing a representative sample of sensors to determine the extent of the problem.

When tests by both the facility and the assessment team indicate that the sensors are reliable, the system can be considered effective for that particular test; however, the testing parameters must be considered. For example, the system may not have been tested for all contingencies, or the test that was used may not have stressed the system to the limit.

Related tests or activities, such as perimeter barrier examinations, tests of CCTV and video-recording equipment, and tests of tamper and line supervision alarms, are typically conducted concurrent with the sensor tests. During these activities, assessors need to look at the integrated system as a whole to determine whether it is effective in defeating intruders. Also, when the results of a test of one element are poor, assessors should determine the impact of that result on the system.

Interior Intrusion Detection and Assessment

Assessors should be aware that many interior sensor systems rely on redundant or layered protection (that is, a combination of barrier, volumetric, and point protection). If testing reveals deficiencies in any one of these, the results should be closely examined in light of program objectives and the complementary systems.

Entry and Search Control/Badges, Passes, and Credentials

Deficiencies in the badge system that can result in unauthorized personnel gaining access to classified information, security areas, or vital equipment are significant. Assessors should pay particular attention to the effectiveness of control over the life cycle of the badge, including procurement, storage, issuance, disposition, and recovery. Other deficiencies in the badging system may include network and operational vulnerabilities.

Significant deficiencies in the badge system may indicate inadequate management attention, training, or resources devoted to administering and maintaining the badge system. All deficiencies should be evaluated to determine whether they result from human error, a systemic procedural problem, or a lack of supervisory emphasis. The root cause of any significant problem should be determined.

Barriers

While barriers cannot absolutely preclude an adversary gaining entry into the area being protected, they should provide delay times and, when properly complemented by IDSs, notification in the event of an attempted penetration. The lack of effective barriers may affect response times and may place an undue reliance on other systems.

Communications

The absence of adequate communication systems or duress alarms significantly impacts the capabilities of the protective force. One of the most important factors in an effective system is ensuring that the protective force responds to intrusion or duress in a timely and effective manner. To be able to respond appropriately, they must be able to communicate with the alarm stations, guard posts, response forces, and LLEAs. Inadequate communication systems may result from budget constraints, lack of planning, or lack of management attention.

Testing and Maintenance

The backbone of any PSS is the testing and maintenance program. Without testing, alarm response and system reliability cannot be measured with any degree of certainty. Without maintenance, the hardware associated with these systems will begin to fail and, ultimately, deteriorate. The lack of an effective testing and maintenance program is a significant deficiency and is usually the root cause of a number of other problems. If this program is deficient, there likely are problems in training, service, repair, or management support.

Support Systems

All critical security systems that operate on electrical power must have a backup power source. These systems include:

- IDS equipment
- CCTV
- Access controls
- Fixed base station communications equipment
- Alarm annunciation equipment
- Security lighting.

Failures in these backup sources may indicate an isolated mechanical problem or a systemic weakness in either the system or the testing and maintenance program.

If "load shedding" is required because auxiliary power sources cannot instantaneously accept the full load of security equipment, the rationale for sequencing the load should be assessed. For example, the most critical loads, such as alarms and communications equipment, should be picked up first, followed by the less-critical systems, such as CCTV systems and lighting.

When assessing batteries, it is important to remember that many batteries have a predictable useful life, after which rapid degradation followed by complete failure can be expected. If all batteries were installed at the same time, it is likely that failure will occur in rapid succession throughout the system.

If there are indications that an adversary could defeat tamper protection without being detected in a significant number of attempts, the tamper-protection system likely is unreliable. This situation should be analyzed in light of site-specific protection objectives and the effectiveness of complementary systems.

If there are indications that one or more tamper or line supervision devices are not functioning, it may be an isolated instance of component failure or an indication of systemic deficiencies in the design of the system.

Contractor and DOE Field Element Performance

PSS assessors should consider both contractor performance and DOE field element performance. In evaluating contractor performance, the PSS team should consider:

- Compliance with DOE orders, including the number and significance of findings in site office surveys and EA assessments
- Responsiveness, indicated by procedures and timeliness in addressing and closing out previous findings
- QA program effectiveness, reflected by the quality of documentation, plans, procedures, records, and internal audit programs
- Defense-in-depth, including the number of layers of protection and the deployment of complementary systems
- Use of testing and maintenance records and false and nuisance alarm records to enhance system performance.

In evaluating DOE field element performance, the PSS team should consider whether:

- Surveys addressing PSS are current.
- Survey findings are consistent with the survey report narrative and work papers.
- Previous EA PSS assessment concerns have been addressed.
- Survey results have been communicated to the facility operating contractor so that corrective actions can be implemented.
- Survey findings are tracked to completion and resolved in a timely manner.
- Exceptions are appropriate and documented.

Where appropriate, the assessment report should specifically identify weaknesses associated with contractor performance. Similarly, weaknesses specific to DOE line management should be identified as such.

Consideration of ISSM Concepts

EA does not use the guiding principles or core functions of ISSM directly as a basis for findings. However, the ISSM concept provides a useful diagnostic framework for analyzing the causes of identified deficiencies. For example, assessors may find that a required action is not being completed. Upon further investigation, assessors may determine that the reason is that there has not been clear designation of responsibility for completing the required action. This situation may indicate a weakness related to line management responsibilities. In such cases, the assessors would cite the deficient condition (i.e., the failure to complete the required action) as the finding and reference the requirement. In the discussion and opportunities for improvement, however, the assessors may choose to discuss the general problem with assignment of responsibilities as a contributing factor.

As part of the analysis process, PSS assessors should review the results (both positive aspects and weaknesses/findings) of the review of the PSS topic in the context of the ISSM concept. Using this diagnostic process, assessors may determine that a number of weaknesses at a site or particular facility may have a common contributing factor that relates to one or more of the management principles. For example, a series of problems in intrusion detection effectiveness could occur if line management has not placed sufficient priority on testing and maintenance and has not provided adequate resources to implement an effective maintenance program. In such cases, the analysis/conclusions section of the PSS appendix of the assessment report could discuss the weaknesses in management systems as a contributing factor or root cause of identified deficiencies.

Appendix A: Intrusion Detection System Performance Tests

Part 1

Exterior Perimeter Sensors

Part 1

Exterior Perimeter Sensors

Objective

The objective of these performance tests is to determine the effectiveness of exterior perimeter sensors.

System Tested

System: Intrusion detection system (IDS)

Function: Perimeter-intrusion detection

Component: Exterior sensors, transmission lines, alarm processing equipment, interfaces with closed circuit television (CCTV) and central alarm station (CAS) operation, testing and maintenance of perimeter sensors.

Scenario

Assessors should select one or more zones of a perimeter system for testing based on sensor configuration, terrain, location of buildings and portals, and operating history. A tour around the perimeter is helpful in identifying zones and potential deficiencies. Items of interest may include ditches, humps, dips, other terrain variations, obstacles or obstructions, sewer lines, pipes or tunnels that pass under the zone, piping or utility lines that pass over the zone, barriers that could be used as a platform to jump over sensors or to avoid observation, excessive vegetation, and standing water. Particular attention should be paid to the identification of potential gaps in sensor coverage.

The number of sensors and zones selected for testing depends on the time available, the importance of the system in the overall protection program, and the variation in the individual zones. The following guidelines are intended to assist the assessor in the selection of sensors and zones for testing:

- A sufficient number of zones and sensors should be tested to provide an adequate indication of the effectiveness of the IDS. If the zones employ different sensor configurations, or if the sensor configuration at portals is significantly different, the assessors should consider selecting at least one of each configuration type.

- Each type of sensor should be tested, if possible. Potential test locations may include areas where sensor zones overlap, as well as areas around portals, buildings, and wall roofs. Additionally, sensors (if any) in tunnels under and structures over the perimeter should be evaluated.

- If the first few performance tests do not indicate problems and there is no evidence of exploitable deficiencies, the assessors generally should not devote extensive time to testing numerous zones and sensors. However, if deficiencies are apparent, the assessors should collect sufficient data to determine whether a deficiency is an isolated instance or evidence of a systemic problem.

- Tests should be conducted for selected zones in which terrain features or questionable installation practices are likely to degrade detection capability.

It is useful for assessors to observe security alarm technicians or security police officers (SPOs) conducting routine operational or sensitivity tests. Assessors should determine whether the tests, calibrations, and maintenance procedures are consistent with U.S. Department of Energy (DOE) orders and the Site Safeguards and Security Plan (SSSP), and whether they are an effective means of testing the systems. Two goals are accomplished by having the facility's security technicians conduct the routine test prior to testing by the assessors. First, the facility tests are indicators of the effectiveness of the test and maintenance program and procedures. Second, the facility tests should verify that the sensors are calibrated according to facility specifications to ensure that assessors will be testing a system that is operating as the facility intends. Consistency with DOE orders and the SSSP may be important in identifying the root cause of any deficiency.

The assessors may conduct walk tests, crawl tests, run tests, jump tests, climb tests, and step tests, as appropriate, to determine whether an adversary could cross the perimeter without detection and whether the sensitivity settings of individual sensors are properly adjusted.

Assessors should monitor the alarm annunciation in the CAS and secondary alarm station (SAS) to determine whether the alarms are functioning properly. The assessors should also observe the operation of interfacing systems such as the automatic CCTV display and video recorders.

Evaluation

If the detection system is effective, the sensors will detect intrusion and the alarms will annunciate accordingly.

Evaluating Sensor Performance

The primary objective in the evaluation of exterior perimeter intrusion detection sensors is to determine whether the system effectively and reliably detects an intruder crossing the perimeter. The following questions should also be considered in the evaluation:

- Do the individual sensors detect an individual crossing the sensor detection pattern at varying rates? Typically, the slowest rate for testing should be .15 meter per second and the fastest rate should be 5 meters per second. However, if patrol frequencies and direct visual observation are considered inadequate to reasonably ensure that such attempts would be detected, speed is no longer relevant.

- Are the sensors positioned to allow adversaries to bypass one sensor at a time, or are they positioned such that an adversary attempting to bypass one sensor would be in the detection zone of a second (and possibly a third) type of sensor?

- Does the alarm system annunciate all alarms, or does the system incorporate alarm processing logic (for example, one of two, two of three, two of four) that allows one sensor or sensors in different zones to activate without an alarm condition? If so, can adversaries exploit the design (i.e., can adversaries cross the perimeter without causing an alarm)? The assessors should consider tactics such as zone hopping and defeating one of two complementary sensors.

- Can the adversary exploit the existing barriers (for example, fences, jersey bouncers) as a platform for jumping or as an aid in climbing to avoid detection?

- Have effective measures been taken to eliminate potential paths under (for example, storm sewers) or over (for example, wires or pipes) the detection zone?

- Are there any seams or bypasses between zones that can be exploited? If so, and if there are multiple sensors, can more than one sensor be defeated?

- Are there dips, ditches, humps, or obstructions that could provide a pathway for an individual to avoid detection? If so, can those deficiencies be identified from outside the secure area?

- Are there probable differences in the day and night detection capability due to extremes of heat and cold or effects of sunlight versus darkness?

- Is the detection zone free of snow, ice, standing water, vegetation, or other obstructions that could prevent detection or cause nuisance alarms?

- Are sensors accessible from outside the Protected Area, making them vulnerable to tampering (for example, “nudging” sensors out of alignment, jamming multiple infrared or microwave sensors, blocking CCTV cameras)?

- Are the sensors particularly susceptible to defeat by adversaries using tools (for example, ladders, boards, ropes)?

Interpreting Results

The following guidelines are provided to assist the assessors in interpreting results in the context of system performance.

- A perimeter system is only as good as its weakest link. Tests that indicate that a knowledgeable adversary could frequently cross the perimeter without detection in one or more zones are evidence that the perimeter sensors are not a reliable system. The significance of this finding must be analyzed in the context of the site-specific protection objectives and the effectiveness of other complementary systems.

- In some cases, testing by assessors indicates that one or more sensors can be defeated but that, because of the degree of redundancy in the sensor configuration, an intruder crossing the perimeter would cause an alarm. In such cases, the identified deficiencies are of lesser concern because the tests indicate the combination of sensors is effective. However, the sensor deficiencies may indicate testing and maintenance problems.

- In some cases, facility tests indicate that the system is correctly calibrated but tests conducted by an assessor indicate that the sensors can be defeated or do not reliably detect intrusion. In those instances, there likely are deficiencies in the test and calibration procedures and potentially in the quality assurance program.

- Facility tests that indicate that the sensors are calibrated according to specification, in conjunction with tests by assessors that confirm the sensors are capable of reliably detecting an intruder, usually signify that the tested portion of the system is effective and that test and maintenance procedures are effective. However, the limitations of the tests must be recognized. For example, not all methods of defeat, such as bridging of microwave sensors, may have been evaluated.

- Facility tests that indicate that one or more sensors are not calibrated according to specifications may simply be an indication of an isolated instance of sensor drift. On the other hand, this may indicate systemic problems in the test and maintenance program, or problems related to the age and overall condition of the sensor system. If the facility tests indicate sensors are out of calibration, assessors should consider instructing the facility technicians to test a representative sample of sensors to determine the extent of the problem.

Special Considerations

Some types of sensors are sensitive to the size of the intruder (or more accurately, the radar cross-section). Assessors should request that the facility provide a relatively small person to conduct the crawl tests.

Related tests or activities, such as perimeter barrier examinations, tests of CCTV and video-recording equipment, and tests of tamper and line supervision alarms, are typically conducted concurrent with the sensor tests.

Responsibilities

Assessors: Select zones and sensors. Direct tests and monitor alarm annunciation. (Typically one assessor will be stationed at the CAS and at least one at the perimeter.)

Facility: Conduct routine tests. Provide security technicians. Provide test devices as necessary (for example, aluminum spheres). Provide SPOs for security during testing, as required. Provide radios for two-way communication. Provide personnel (normally an SPO) to conduct tests (climb, crawl, run, and walk) at the direction of assessors.

Internal Coordination

Tests should be scheduled to avoid conflicts with other tests involving the protective force.

Security Considerations

All normal security precautions should be taken. Normally, an SPO should be present to observe testing to ensure that there is no unauthorized access or activity at the protected location to be tested. In many cases, special security arrangements must be made before accessing exterior locations where security sensors are located. These arrangements should be coordinated in advance to avoid delays during the testing.

Personnel Assignments

Test Director:

Facility Alarm System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- Alarm technicians
- Tester(s)
- SPOs to provide security during tests, as necessary.

Equipment:

- Radios
- Physical security systems test kit and devices: Assessors should have an understanding of how the physical security systems test kit/devices are used, including:
    - Test kit shipping and receiving procedures for shipment to assessed sites
    - Application and functionality of test kit devices (e.g., aluminum sphere for microwave and calibrated punch for fence vibration sensors, infrared target simulator, glass-break detector, audio source)
    - Preparing testing devices for exterior or interior performance testing
    - Regular preventive maintenance for the test kit devices (e.g., battery replacement, calibration, lifecycle limitations).

Safety:

- Follow normal operating procedures.
- Complete safety plan.
- Notify CAS and other alarm monitoring stations before testing.
- Station one assessor in the CAS.
- Coordinate with protective force personnel to prevent any undesired armed response.
- Use personal protective equipment.

Bistatic Microwave Sensors

General Characteristics: Line-of-sight, freestanding, transmitter/receiver pairs

Intruder Detection Capabilities: Walking, slow walking, running, crawling, rolling, climbing, and jumping

Vulnerabilities: Tunneling, trenching, bridging, pass through

Concerns

- Level terrain over the length of the detection zone is critical. Ditches, humps, or dips greater than three inches may significantly reduce the capability to detect a crawling intruder.

- Insufficient offset may allow intruders to crawl under or jump over the beam at the crossover point (the point where adjacent zones overlap; typically, 30 feet or more is required).

- Separation distances between the transmitter and receiver that are greater than the effective range of the detector (typically 100 meters) may significantly reduce detection capability.

- Microwave sensors are susceptible to nuisance alarms induced by movement of standing water, blowing debris, and blowing snow; movement of animals and lightning; and movement of fencing that is located within the sensor detection zone. Properly drained terrain and well-maintained isolation zones (vegetation free and without holes that would allow large animals to enter) can reduce the nuisance alarm rate.

- The accumulation of snow may reduce sensor performance.

- Improper alignment may significantly reduce sensitivity and detection width, and contribute to false alarms.

- Transmitters or receivers that are mounted too high may not detect someone crawling under the sensor.

- Transmitters or receivers that are mounted close to the ground may not detect someone vaulting over at the crossover point, if there is insufficient overlap between adjacent zones.

- Dumpsters, shipping crates, trash cans, and electrical boxes can create dead spots that are ideal areas for intrusion attempts. In addition, signals reflected from these objects can extend sensor coverage to areas not intended to be covered, possibly creating false alarms.

- Areas that contain strong emitters of electric fields (radio transmitters) or magnetic fields (large electric motors or generators) can cause areas of decreased sensitivity.

Types of Tests

- Walk Test Across the Zone

  Walk tests or shuffle walk tests are conducted to verify operability and sensitivity, and to determine the width of the detection zone. A shuffle walk involves small slow steps without swinging the arms, steps of five centimeters (cm) or less moving at .15 meters/second (m/sec). The width of the detection zone can be determined by monitoring alarm annunciation. Sensitivity tests should be conducted at various points including the mid-range of the sensor beam.

- Walk Test Parallel to the Zone

  Walk tests parallel to the zone are conducted to determine whether the sensor is misaligned or mounted too close to the fence. Such tests involve walking parallel to the zone approximately one meter from the fence and verifying that no alarm occurs.

- Run Tests

  Run tests are conducted to verify whether receiver response is fast enough. Run tests involve crossing the detector zone at a fast run (5 m/sec). Such tests are performed where the beam is narrow – approximately six meters from the transmitter or receiver or just inside the crossover point (for overlapping sensors).

- Climb Over Tests

  Climb over tests are conducted to verify that adequate detection height and width is achieved on climbable ground and aerial structures located in the alarm detection zones. These structures include vehicular and pedestrian portal fence top rails, sides or rooftops of buildings, or utilities that may pass over the sensor bed.

- Jump Tests

  Jump tests are conducted to verify adequate detection height. Such tests involve attempting to jump over the beam and are conducted where the beam is narrowest (typically near the crossover point). Barriers, buildings at the perimeter, sensor posts, or mountings may be used as platforms for jumping.

- Crawl Tests

  Crawl tests are conducted to verify proper detector alignment and sensitivity, and to determine whether terrain irregularities can be exploited. Crawl tests involve crossing the detection zone at selected points while minimizing radar cross section (intruder remains flat, parallel to the beam, head down, with no reflective clothing). Tests should be conducted by a relatively small individual crawling at approximately .15 m/sec. Tests should be conducted at various points along the detection zone, including just inside the crossover point, at the mid-range, and wherever terrain features are likely to impede detection.

Test Guidelines

- All tests listed in the previous section should be conducted on at least two typical zones.

- Zones that are substantially different (different terrain, sensor configuration, portals) should also be considered for testing.

- Areas that appear vulnerable (due to alignment, terrain irregularities, or other concerns) should be tested.

- If an individual sensor can be defeated, that same sensor should be retested to determine whether it can be defeated a second time. Several tests of the same sensor may be required to determine whether an adversary can exploit the sensor.

- If an individual microwave sensor can be defeated by one or more methods (for example, jump, run, and crawl), the microwave sensors in other zones should be tested using the same methods in order to determine the extent of the problem. Assessors should conduct several (three to five) more tests in different zones. If most of these tests indicate that the sensor can be reliably defeated, there is sufficient evidence of a systemic

problem. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If the results are inconclusive, assessors should consider testing additional sensors. Only rarely would an assessor test more than 10 to 15 zones.

- If the adversary has the knowledge, time, and equipment, bridging or tunneling can defeat all microwave sensors. Such tests should only be conducted if a zone is particularly vulnerable (for example, due to barrier placement, or if patrol frequencies and direct visual observation are considered inadequate to reasonably ensure that such attempts are detected).

- Experience with microwave sensors indicates that the slowly crawling intruder and the intruder jumping over a single stack microwave unit are the most difficult to detect. Therefore, much of the testing effort is devoted to crawl tests along with assisted and unassisted jump tests in microwave zones that appear to have alignment problems or terrain irregularities.

Checklist

Bistatic Microwave Sensors

Exterior Perimeter IDS

Interview Items

Installation location: ____

____

Operational test frequency: ____

____

Operational test method: ____

____

Sensitivity test frequency: ____

____

Sensitivity test method: ____

____

Acceptance criteria for sensitivity test: ____

____

Procedures for vegetation removal: ____

____

Procedures for snow removal: ____

____

False alarm history/records: ____

____

Make/model: ____

____

Measures to prevent erosion: ____

____

Tamper switches (transmitter, receiver, junction boxes): ______________________________

____

Tour/Visual Examination Items

Vegetation present? ____

____

Deep snow present? ____

____

Terrain level? ____

____

Zone length OK? ____

____

Complements other sensors? ____

____

Overlap sufficient? ____

____

Standing water present or likely? ____

____

Frequency of patrols? ____

____

Data Collection Sheet
Bistatic Microwave – Exterior Perimeter IDS

Test Method

	Zone Tested	Zone Number	Walk Across	Walk Shuffle	Walk Parallel	Run	Crawl	Jump
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								

Comments:

Active Infrared Sensors

General Characteristics:	Line-of-sight, vertical plane, post-mounted, multiple transmitters and receivers
Intruder Detection Capabilities:	Walking, slow walking, running, crawling, rolling, jumping
Vulnerabilities:	Tunneling, trenching, bridging, climbing

Concerns

- Because infrared is a narrow beam line-of-sight detector, there should be no surface depressions of six inches or more that may permit crawling under the lowest transmitter/receiver pair. The bottom beam should be aligned within six inches of the ground surface.
- The ground under the detection zone should be compacted, graveled, or paved to preclude easy burrowing under the zone (loose gravel is usually a significant problem).
- Close proximity to fences, building walls, CCTV towers, or other structures may permit easy bridging or jumping over the narrow vertical detection zone (sensor stacks can become climbing aids).
- Infrared sensors are susceptible to nuisance alarms induced by animals, vegetation, fog, snow, and wind-blown dust and debris.
- Heavy snow should be removed to preclude tunneling through the snow to avoid detection.
- In some older-model sensors, sunlight and vehicle headlights may cause false alarms.
- Improper alignment may reduce sensitivity and detection width, and contribute to nuisance alarms.

Types of Tests

- Walk Test Across the Zone

  Walk tests are conducted to verify operability and sensitivity. These tests should be conducted at mid-range of the sensor beam.

- Run Tests

  Run tests are conducted to verify that receiver response is fast enough. They involve crossing the detector zone at a fast run (5 m/sec).

- Crawl Tests

  Crawl tests are conducted to verify proper detector alignment and sensitivity, and to determine whether terrain irregularities can be exploited. Crawl tests involve crossing the detection zone at selected points while minimizing target cross-section (intruder remains flat, perpendicular to the beam, head down, with no reflective clothing). Tests should be conducted by a relatively small individual moving at approximately .15 m/sec). Tests should be conducted at various points along the detection zone, including the mid-point and wherever terrain features are likely to reduce detection capability.

- Jump Tests

  Jump tests are conducted to verify adequate detection height. Such tests involve attempting to jump over the beam and are conducted where barriers, buildings, sensor posts, or mountings can be used as jumping platforms.

Test Guidelines

- All the tests listed in the previous section should be conducted on at least two typical zones.

- Zones that are substantially different (different terrain, sensor configuration, or portals) should also be considered for testing.

- Areas that appear vulnerable (due to structures that aid bridging or jumping, terrain features, or other concerns) should be tested.

- If an individual sensor can be defeated, that same sensor should be tested again to determine whether such defeat can be repeated. Several tests of the same sensor may be required to determine whether an adversary can reliably exploit a sensor deficiency.

- If an individual zone can be defeated by one or more methods (for example, jump, run, crawl), other zones should be tested using the same methods to determine the extent of the problem. The assessors should conduct several (three to five) more tests in different zones. If most of these tests indicate that the sensor can be reliably defeated, there likely is a systemic problem. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If results are inconclusive, the assessors should consider testing additional sensors. Only rarely would an assessor test more than 10 to 15 zones using the same methods.

- If the adversary has the knowledge, time, and equipment, bridging or tunneling techniques can be used to defeat infrared sensors. Since the infrared beam employed by these sensors is quite narrow, bridging or tunneling can be accomplished rapidly and easily. Tests to evaluate bridging or tunneling should only be conducted in locations that are particularly vulnerable to defeat (for example, due to adjacent barrier placement) or if patrol frequencies and direct visual observation (CCTV or guard posts) are considered inadequate to reasonably assure that attempts to defeat these sensors will be detected.

- Experience with infrared sensors indicates that jumping the zone at the mounting post is the most likely method of quickly defeating the system. This method, together with the crawl test (where there are depressions in the ground surface), should be used when possible in testing activities.

Checklist

Active Infrared Sensors

Exterior Perimeter IDS

Interview Items

Installation location: ____

____

Operational test frequency: ____

____

Operational test method: ____

____

Sensitivity test frequency: ____

____

Sensitivity test method: ____

____

Acceptance criteria for sensitivity test: ____

____

Procedures for vegetation removal: ____

____

Procedures for snow removal: ____

____

False nuisance alarm history/records: ____

____

Make/model: ____

____

Measures to prevent erosion: ____

____

Tamper switches (transmitter, receiver, junction boxes): ____

____

Tour/Visual Examination Items

Vegetation present? ____

____

Deep snow present? ____

____

Terrain level? ____

____

Zone length OK? ____

____

Complements other sensors? ____

____

Overlap sufficient? ____

____

Structures adjacent to the zone permitting vaulting/bridging? ____

____

Data Collection Sheet
Active Infrared Sensors – Exterior Perimeter IDS

Test Method

	Zone Tested	Zone Number	Walk	Run	Crawl	Jump	Bridge
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							

Comments:

Electric Field Sensors

General Characteristics: This sensor consists of electric field-generating wires and sensor wires. These sensors can be installed on freestanding posts or they can be fence-mounted. Either configuration has the unique feature of following irregular terrain.

Intruder Detection Capabilities: Walking, slow walking, running, crawling, rolling, jumping

Vulnerabilities: Tunneling, trenching, bridging

Concerns

- Improper wire/spring tension or improper wire/insulation coupling can cause unacceptable false and nuisance alarms. Careful installation and maintenance are required for proper sensor operation.

- Two-wire (versus three- or four-wire) configurations may permit an intruder to jump between the field wire and sensing wire undetected.

- In locations where more than one section of electric field is installed, adjacent sensors should overlap to overcome the lack of sensitivity around the tension springs and end insulators.

- Electric field sensors are not generally used at fence gates because of the requirement to maintain wire tension, although removable sections can be used. For frequently used gates, active infrared or microwave sensors are normally used. In such cases, there must be sufficient overlap between the gate sensor and the adjacent electric field zone to preclude intrusion between zones of different sensors.

- Electric field sensors are susceptible to nuisance alarms from lightning, high-level electromagnetic noise (for example, transformers), moving animals, heavy rain, wet snow, and blowing debris.

- These sensors may not provide adequate coverage in locations where there are washouts in the sensor bed.

Types of Tests

- Walk Test Perpendicular to the Zone

  Walk tests are used to verify sensor operability and sensitivity. The zone should alarm when approached at normal walking speed when the tester is between 1 and .5 m from the wire (see Evaluating Sensor Performance, page PSS-90).

- Shuffle Walk Test Perpendicular to the Zone

  Shuffle tests are conducted by taking slow, small steps without swinging the arms (steps of 5 cm or less at .15 m/sec). The system should alarm at a distance of 25 cm or less, and any attempt to climb between the wires should be detected.

- Stoop Test (for four-wire systems)

  This test is conducted by walking to a point near the sensor, then facing parallel to the wires. The control unit should be allowed to stabilize, and then the individual should stoop or squat down to unbalance the upper and lower zones. An alarm should annunciate as a result of this action.

- Crawl Test Perpendicular to the Zone

  The crawl test consists of an individual crossing the zone at a slow crawl as close to the ground as possible, in zones where the bottom wire is highest (6 inches or more) from the ground or where there is a depression in the zone. An alarm should annunciate as a result of this action.

- Jump Test

  The jump test cannot normally be performed due to the height of the detection zone (eight feet or more) if the electric field sensor is properly installed. However, where there are structures with adequate height adjacent to the zone, it may be possible to jump over the sensor wire, if personal safety can be ensured.

- Step-Through Test

  Step-through tests should be conducted if the walk tests, shuffle walk tests, and stoop tests indicate that the electric field sensors are not sufficiently sensitive. The step-through test consists of an individual stepping or jumping between the electric field wires and crossing the detection zone while avoiding contact with the wire. If the zones do not overlap, this test should be conducted at the start or end of the zone (near tension springs) where sensitivity is lowest. Otherwise the test should be conducted at several locations throughout the zone. Some of the older models are more susceptible to penetration.

Test Guidelines

- The person conducting the tests should remove all metal objects and should not wear steel-toed shoes or wear gloves.

- Walk tests, shuffle walk tests, and crawl tests should be conducted on at least two typical zones.

- If sensitivity is questionable on the initial walk or stoop tests, the step-through tests should be conducted to determine whether a person can cross the detection zone undetected.

- Zones that are substantially different (different terrain, sensor configuration, portals) should also be considered for testing.

- Areas that appear vulnerable (due to terrain features or other concerns) should be tested (crawl tests or jump tests).

- If an individual sensor can be bypassed, that same sensor should be tested again to determine whether bypassing can be repeated. Several tests of the same sensor may be required to determine whether an adversary can reliably exploit the sensor deficiency.

- If an individual electric field zone can be defeated by one or more methods (for example, jumping, running, crawling), other zones should be tested using the same methods to determine the extent of the problem. The assessors should conduct several (three to five) more tests in different zones. If most of these tests indicate that the sensor can be reliably defeated, there likely is a systemic problem. If no other sensors are defeated, it may be concluded that an isolated deficiency was identified. If the results are inconclusive, additional sensors may be considered for testing. Only rarely would an assessor test more than 10 to 15 zones using the same method.

- If an adversary has the appropriate knowledge, time, and equipment, bridging or tunneling techniques can defeat any electric field sensor. Tests to evaluate these defeat methods should only be conducted if specific zones are vulnerable because patrol frequencies and direct visual observation (CCTV or guard posts) are inadequate to reasonably ensure that those defeat attempts are detected.

- Experience with electric field sensors indicates that the slow-crawling intruder is the most difficult to detect. Typically, much of the test effort associated with this sensor type is devoted to crawl tests of zones that appear to have irregular terrain.

Checklist

Electric Field Sensors

Exterior Perimeter IDS

Interview Items

Installation location: ____

____

Operational test frequency: ____

____

Operational test method: ____

____

Sensitivity test frequency: ____

____

Sensitivity test method: ____

____

Acceptance criteria for sensitivity test: ____

____

Procedures for vegetation removal: ____

____

Procedures for snow removal: ____

____

False alarm history/records: ____

____

Make/model: ____

____

Measures to prevent erosion: ____

____

Tamper switches (transmitter, receiver, junction boxes): ____

____

Tour/Visual Examination Items

Vegetation present? ____

____

Deep snow present? ____

____

Terrain level? ____

____

Zone length OK? ____

____

Complements other sensors? ____

____

Overlap sufficient? ____

____

Wire tension and terminations satisfactory? ____

____

Data Collection Sheet
Electric Field Sensors – Exterior Perimeter IDS

Test Method

	Zone Tested	Zone Number	Walk	Walk Shuffle	Stoop	Crawl	Jump	Step Through
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
Comments:								

Buried Line Sensors

General Characteristics:	Buried cable(s); seismic, magnetic, or electromagnetic coupled field detectors; ported coax; cable(s) follow terrain
Intruder Detection Capabilities:	Varies depending on type; may include walking, running, jumping, crawling, trenching, and tunneling
Vulnerabilities:	Bridging techniques employed by a potential intruder and decreased sensitivity resulting from standing water

Note: Due to the varying sensing techniques of buried line sensors, the strengths and weaknesses of various systems differ somewhat. However, the method of testing is the same for each.

Concerns

Standing water, wind-blown debris, electromagnetic interference, vehicular traffic, lightning, and animals may cause nuisance alarms.

- Seismic sensors may not function when installed under roadbeds or sidewalks, or when the ground is frozen or under deep snowpack.
- Ported "leaky" coax is susceptible to nuisance alarms resulting from moving water, moving metallic objects such as vehicles, and lightning.
- Seismic sensors may experience nuisance alarms if installed in the vicinity of fences, power poles, guy wires, or roads (vehicle ground vibration).
- Ground covering the sensor should be maintained in such a manner that the actual location of the sensor is not visually apparent.

Types of Tests

- Walk Tests Across the Zone

  Walk tests should be conducted at a normal walking speed in at least three places within each buried cable zone.

- Run or Jump Tests Across the Zone

  Run tests are conducted to verify prompt sensor response and should be conducted at a fast run (5 m/sec) at three locations within a given detection zone. The runner may attempt to jump over the location where the sensor is buried.

- Roll Tests to the Zone

  Roll tests consist of an individual slowly rolling across the detection zone with the body oriented parallel to the buried cable(s) with arms held close to the body and legs together. A roll test should be conducted when there is a hard surface road or sidewalk crossing the zone.

Test Guidelines

- All tests listed in the previous section should be conducted on at least two typical zones.

- Areas that appear vulnerable (due to the existence of hard surface roads, standing water, sources of seismic interference, or other reasons) should be tested.

- If an individual sensor can be defeated, that same sensor should be tested again to determine whether it can be defeated again. Several tests of the same sensor may be required to determine whether an adversary can reliably exploit the sensor.

- If an individual zone can be defeated by one or more methods, the buried line sensors in other zones should be tested using the same methods to determine the extent of the problem. Assessors should conduct several (three to five) more tests in different zones. If tests indicate that the sensor can be repeatedly defeated, there likely is a systemic problem. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If the results are inconclusive, additional testing should be considered. An assessor would rarely test more than 10 to 15 zones using the same methods.

- If the adversary has the knowledge, time, and equipment, bridging techniques can defeat most buried line sensors. Such tests should only be conducted if a zone is particularly vulnerable, or if patrol frequencies and direct visual observation (CCTV or guard posts) are considered inadequate to reasonably assure that these attempts will be detected.

Checklist

Buried Line Sensors

Exterior Perimeter IDS

Interview Items

Installation location: ____

____

Operational test frequency: ____

____

Operational test method: ____

____

Sensitivity test frequency: ____

____

Sensitivity test method: ____

____

Acceptance criteria for sensitivity test: ____

____

Procedures for vegetation removal: ____

____

Procedures for snow removal: ____

____

False alarm history/records: ____

____

Make/model: ____

____

Tamper switches (transmitter, receiver, junction boxes): ____

____

Tour/Visual Examination Items

Vegetation present? ____

____

Deep snow present? ____

____

Terrain level? ____

____

Zone length OK? ____

____

Complements other sensors? ____

____

Overlap sufficient? ____

____

Standing water present or likely? ____

____

Hard surfaced road crosses zone? ____

____

Power poles, guy wires, or other seismic sources exist? ____

____

Data Collection Sheet
Buried Line – Exterior Perimeter IDS

Test Method

	Zone Tested	Zone Number	Walk	Run/Jump	Roll
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
Comments:					

Taut-Wire Sensor Fence

General Characteristics:	Tensioned horizontal wires connected to detector posts, freestanding or fence-mounted
Intruder Detection Capabilities:	Cutting, climbing, or other deflection of sensor wire
Vulnerabilities:	Tunneling, trenching, bridging

Concerns

- Since taut-wire sensors operate on mechanical principles, they are relatively impervious to weather, wind, electromagnetic interference, and other common sources of nuisance alarms.

- Some systems that have only one sensor switch channel for multiple parallel switches may be defeated by cutting ungrounded switch leads if the end-of-line resistor and signal cable are not disturbed.

- As with other fence-mounted mechanical (pressure, strain, vibration) sensors, taut-wire systems are susceptible to defeat by tunneling, bridging, or jumping, if no physical contact with the sensing wires occurs.

- Taut-wire sensors are not generally used at fence gates because of the requirement to maintain wire tension. For frequently used gates, active infrared or microwave sensors are often used. In such cases, there must be sufficient overlap between the gate sensor and the adjacent taut-wire zone to preclude intrusion between zones of different sensors.

- Older systems used fewer total wires, allowing assessors to climb over the system or under the system if not fence mounted.

- The system is one of the more reliable fence-based detectors because it is less susceptible to environmental conditions and small animals. However, improper tensioning of the sensors can cause unreliable detection. Varying weather conditions generally will not cause false alarms when the system is properly installed. Typically, small animals do not pose a threat for false alarms either, because a force of about 35 pounds is needed for the sensor to be activated.

Types of Tests

- Simulated Climb Test (for freestanding taut-wire sensors)

  This test consists of a ladder being placed against the wires and an individual climbing the ladder to a point where sensor activation occurs (usually when the knees are near the top of the fence).

- Wire Pull Test

  Individual wires are pulled up or down by hand so that a deflection of approximately four inches is achieved.

- Jump Tests

  These tests cannot normally be performed if the taut-wire sensor is properly installed, due to the height of the detection zone (eight feet or more). However, structures adjacent to the zone used as platforms may make it possible to jump over the sensor wire, if personal safety can be ensured.

- Crawl Tests

  Crawl tests should be conducted in locations where washouts or burrowing is possible.

Note: During periods of extreme cold weather, mechanical sensor switches may take a while to return to the normal neutral position after activation. This delay should be taken into account when considering multiple tests of the same zone.

Test Guidelines

- All tests listed in the previous section should be conducted on at least two typical zones.

- Zones that are substantially different (different terrain, sensor configuration, portals) should also be considered for testing.

- Areas that appear vulnerable (due to terrain irregularities or other reasons) should be tested to determine whether there is a vulnerability.

- If an individual sensor can be defeated, that same sensor should be tested again to determine whether it can be defeated repeatedly. Several tests of the same sensor may be required to determine whether an adversary can reliably exploit the sensor deficiency.

- If an individual taut-wire zone can be defeated by one or more methods (for example, bridging and climbing), other zones should be tested using the same methods to determine the extent of the problem. Assessors should conduct several (three to five) more tests in different zones. If most of these tests indicate that the sensor can be reliably defeated, there likely is a systemic problem. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If results are inconclusive, additional testing should be considered. Only rarely would an assessor test more than 10 to 15 zones using the same methods.

- If the adversary has the knowledge, time, and equipment, bridging or tunneling techniques can defeat all taut-wire sensors. Such tests should be conducted only if a zone is particularly vulnerable (for example, due to barrier placement), or if patrol frequencies and direct visual observation (CCTV or guard posts) are considered inadequate to reasonably assure that such attempts are detected.

Checklist

Taut-Wire Sensor Fence

Exterior Perimeter IDS

Interview Items

Installation location: ____________________

____

Frequency of operational test: ____________________

____

Operational test method: ____________________

____

Sensitivity test frequency: ____________________

____

Sensitivity test method: ____________________

____

Acceptance criteria for sensitivity test: ____________________

____

Procedures for vegetation removal: ____________________

____

Procedures for snow removal: ____________________

____

False alarm history/records: ____________________

____

Make/model: ____________________

____

Measures to prevent erosion: ____

____

Tamper switches (junction boxes): ____

____

Tour/Visual Examination Items

Vegetation present? ____

____

Deep snow present? ____

____

Terrain level? ____

____

Zone length OK? ____

____

Complements other sensors? ____

____

Overlap sufficient? ____

____

Wire tension and terminations satisfactory? ____

____

Data Collection Sheet
Taut-Wire Sensor Fence – Exterior Perimeter IDS

Test Method

	Zone Tested	Zone Number	Simulated Climb	Wire Pull	Cutting	Jump
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						

Comments:

Video Motion Detection

General Characteristics:	Comparison of digitized camera view with stored video image, some systems have masking capability
Intruder Detection Capabilities:	Any intruder motion affecting a sufficient part of the camera's field of view
Vulnerabilities:	Extreme slow motion and an individual wearing clothing that matches the background

Concerns

- Video motion detectors (VMDs) are complex devices requiring extensive maintenance and adjustment.
- As analytics are added to reduce false alarm rates, detection weaknesses may be introduced.
- Due to high detection sensitivity, some systems are susceptible to nuisance alarms from reflected light, cloud motion, sunrise and sunset, automobile headlights, wind-blown objects, and animals (if the detector's field of view is wide and encompasses areas outside the potential space, the potential for nuisance alarms is greater).
- Camera vibration due to wind may create false alarms, as well as improper camera signal synchronization or other video signal disturbance.
- Camera image tube "burn in" caused by a constant view of the same scene may degrade sensitivity of the VMD, particularly where extreme changes in light to dark contrast are present.
- Any obstruction that blocks the camera's field of view, or creates strong shadowed areas, may prevent intruder detection.
- If the length of the field of view is too long for the camera lens, an intruder at the extreme end of the field of view may be able to avoid detection.
- If the "refresh rate" (the rate at which one camera scene is compared to the previous scene) is too slow, an intruder may be able to run through the field of view near a camera without detection.
- In the case of digital systems, the zone(s) of detection should be reviewed to ensure proper coverage in the field of view.
- Fog or smoke (grenade) is likely to adversely impact system effectiveness.

Types of Tests

- Walk Test Across the Zone

  Walk tests or shuffle-walk tests are conducted to verify operability and sensitivity, and to determine the width of the detection zone. A shuffle walk involves small slow steps without swinging the arms (steps of 5 cm or less at .15 m/sec). Width of the detection zone can be determined by monitoring alarm annunciation. Sensitivity tests should be conducted at the furthermost observable point in the camera's field of view (see Evaluating Sensor Performance, page PSS-90).

- Run Tests

  Run tests are conducted to determine whether the detector response is fast enough. Run tests consist of an individual crossing the detector zone at a fast run (5 m/sec). Such tests are performed at the nearest and furthermost points in the camera's field of view (see Evaluating Sensor Performance, page PSS-90).

- Crawl Tests

  Crawl tests are conducted to verify proper detector sensitivity and to determine whether terrain irregularities can be exploited. Crawl tests consist of an individual crossing the detection zone at selected points (intruder remains flat, parallel to the camera's field of view, head down, with no reflective clothing). Tests should be conducted by a relatively small individual moving at approximately .15 m/sec. Tests should be conducted at various points along the detection zone wherever terrain features are likely to reduce detection and at the furthermost observable point in the camera's field of view (see Evaluating Sensor Performance, page PSS-90).

Note: Cameras outside the Protected Area can be manipulated to prevent alarming during intrusion. Special care must be taken when examining a video motion detector system with unprotected cameras.

Test Guidelines

- Tester should be dressed in standard work clothing (e.g., washed denim jeans and jacket).

- Camouflage will assist the tester (snow camouflage in snow or light-colored gravel).

- All tests listed in the previous section should be conducted on at least two typical zones.

- Zones that are substantially different (different terrain, lighting conditions, obstructions) should also be considered for testing.

- Areas that appear vulnerable (due to lighting deficiencies, terrain irregularities, or other reasons) should be tested to determine whether there is a vulnerability.

- If an individual camera's detector can be defeated, that same camera should be tested again to determine whether the deficiency can be repeated. Several tests of the same zone may be required to determine whether an adversary can reliably exploit the deficiency.

- If an individual camera zone can be defeated by one or more methods (running, walking, crawling), the other camera zones should be tested using the same methods to determine the extent of the problem. The assessors should conduct several (three to five) more tests in different zones. If most of these tests indicate the detector can be reliably defeated, there likely is a systemic problem. If no other zones are defeated, one may conclude that an isolated deficiency was identified. If the results are inconclusive, additional testing should be considered. Rarely would an assessor test more than 10 to 15 zones using the same methods.

Checklist

Video Motion Detection

Exterior Perimeter IDS

Interview Items

Installation location: ____

____

Operational test frequency: ____

____

Operational test method: ____

____

Sensitivity test frequency: ____

____

Sensitivity test method: ____

____

Acceptance criteria for sensitivity test: ____

____

Procedures for vegetation removal: ____

____

Procedures for snow removal: ____

____

False nuisance alarm history/records: ____

____

Make/model: ____

____

Measures to prevent erosion: ____

____

Tamper switches (transmitter, receiver, junction boxes): ____________________________

____

Tour/Visual Examination Items

Vegetation present? ____

____

Deep snow present? ____

____

Terrain level? ____

____

Zone length and field of view OK? ____

____

Complements other sensors? ____

____

Overlap sufficient? ____

____

Obstructions present? ____

____

Lighting adequate? ____

____

Data Collection Sheet
Video Motion Detection – Exterior Perimeter IDS

Test Method

	Zone Tested	Functional Test	Walk	Run	Crawl
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
Comments:					

Monostatic Microwave Sensors

General Characteristics:	Volumetric coverage; transmitter/receiver unit; typically mounted pointing at a building to provide coverage of approaches; also used on rooftops or gates
Intruder Detection Capabilities:	Walking, slow walking, running, crawling, rolling, jumping
Vulnerabilities:	Tunneling, trenching, bridging

Concerns

- Microwave sensors are susceptible to false alarms triggered by standing water, high winds, snow, animals, lightning, and fencing that is too close to the sensor beam. Properly drained terrain and well-maintained isolation zones (vegetation free and without holes that would allow large animals to enter) can reduce the false alarm rate.

- Optimum coverage requires direct line of sight. Obstructions such as columns, beams, air-conditioning units, or other large objects may prevent detection.

- Sensor transceivers and control units are subject to physical damage and tampering if they are readily accessible or are not covered by another sensor's detection pattern.

- Sensors are susceptible to false alarms due to moving objects, electromagnetic radiation from sources such as fluorescent lighting, and seismic vibration.

- Proper overlap and coverage must be considered to ensure that an intruder cannot cross over, around, or under the sensor's pattern of coverage.

- The microwave detection beam can easily penetrate glass, wood, wallboard, and plastic. This characteristic can result in false alarms that are generated by moving objects that are located outside the protected space.

- These sensors are most sensitive to targets moving directly toward or away from the transceiver.

- Dumpsters, shipping crates, trash cans, electrical boxes, and other objects that block microwave signals can create dead spots. These dead spots create ideal areas for intrusion attempts. In addition, signals reflected from these objects can extend sensor coverage to areas not intended to be covered, possibly creating false alarms.

- Areas that contain strong emitters of electric fields (radio transmitters) or magnetic fields (large electric motors or generators) can affect the ability of microwave sensors to function properly and should be avoided or compensated for by distinct signal separation.

- Self-generated signal reflection is a common problem caused by improper placement/mounting and can be avoided by positioning the sensor externally and parallel to the wall rather than imbedding it in the wall.

- Also, large metal objects that can reflect the signal and/produce dead spots should be kept out of the detection zone, as should equipment whose operation involves external movement or rotating functions.

Types of Tests

- Sensitivity Walk Test

  Walk tests are used to verify operation and sensitivity of the sensor. This test is performed by slowly walking (1 ft/sec) toward microwave sensors until an alarm is received. This test should establish the far end of the sensor coverage pattern.

- Crossing Walk Test

  This test verifies the ability of the sensor to detect motion along the least sensitive axis of the detection pattern. After the end of the sensor coverage pattern is determined from a sensitivity walk test, a crossing test should be performed by walking across the far end of a microwave zone from various points outside the detection zone. Detection should occur before the tester enters the defined protected space or reaches the protected asset.

- Avoidance Walk Test

  Based on the sensor coverage pattern (oval, wedge, or circle), the assessor should attempt to enter the target zone by walking around the sensor's zone of coverage. This test should verify adequate sensor coverage and overlap to provide detection for the protected space or target/object.

- Crawl Test

  The crawl test should be conducted as close to the sensor head as possible in an effort to crawl under the detection zone.

- Jump Test

  Jump tests should be conducted in the same manner that bistatic systems are tested.

Test Guidelines

- The person conducting the tests should remove all metal objects and should not wear steel-toed shoes. Observers should be requested to stand away from the area being tested to reduce confusion.

- Testing should be conducted on at least two typical zones.

- Any zones that have potential vulnerabilities caused by obstructions or other sources of interference should be tested to determine whether they can be exploited.

- If there are apparent weaknesses in zone coverage or sensor overlap, these should be tested to determine whether sensor coverage could be circumvented.

- Experience indicates that monostatic microwave sensors are most vulnerable to a very slowly moving target entering the detection zone on the least sensitive axis (across the zone for microwave sensors).

- Some sensors have alarm indicator lights built into the sensor head. The assessors may observe these indicators to facilitate testing the coverage pattern or sensor sensitivity. However, the assessors should also verify that an alarm is received in the alarm stations to ensure that the alarm circuit is functional from sensor to annunciation point.

- If an individual sensor can be defeated, that same sensor should be tested again to determine whether the deficiency can be repeated. Several tests of the same sensor may be required to determine whether an adversary can reliably exploit the sensor deficiency.

- If an individual microwave sensor or zone can be defeated, the microwave sensors in other zones should be tested using the same methods to determine the extent of the problem. The assessors should conduct several (three to five) more tests in different zones. If most of these tests indicate that the sensor can be reliably defeated, there likely is a systemic problem. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If results are inconclusive, additional testing should be considered.

Checklist

Monostatic Microwave Sensors

Exterior Perimeter IDS

Interview Items

Installation location: ____

____

Operational test frequency: ____

____

Operational test method: ____

____

Sensitivity test frequency: ____

____

Sensitivity test method: ____

____

Acceptance criteria for sensitivity test: ____

____

Procedures for vegetation removal: ____

____

False alarm history/records: ____

____

Make/model: ____

____

Tamper switches (transmitter, receiver, junction boxes): ____________________________________

____

Tour/Visual Examination Items

Vegetation present? ____

____

Complements other sensors? ____

____

Overlap sufficient? ____

____

Standing water present or likely? ____

____

Obstructions present? ____

____

Data Collection Sheet
Monostatic Microwave Sensors – Exterior Perimeter IDS

Test Method

	Zone Tested	Sensitivity Walk	Crossing Walk	Avoidance Walk	Crawl
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

Comments:

Fence Disturbance Sensors

General Characteristics:	Sensing wires/cables attached to or woven through fence, sonic capacitance, or piezoelectric technologies
Intruder Detection Capabilities:	Cutting, climbing, or other vibration/deflection of sensor wire or fence
Vulnerabilities:	Tunneling, trenching, bridging

Concerns

- Fence disturbance sensors are susceptible to defeat by tunneling, bridging, or jumping, if no physical contact with the sensing wires occurs.
- Depending on the sensitivity setting, fence disturbance sensors may be susceptible to high false alarm rates. Common causes of false alarms include high winds, moving animals, and other sources of fence vibration. Fences, gates, outriggers, and barbed wire should be mechanically sound and well maintained to prevent excessive fence vibration. Also, signs attached to the fence are often a source of nuisance alarms.
- In some sensor designs, the sensing wires are least sensitive near the terminal connections and corners.
- The sensor wire or sensors must contact the fence for reliable, nuisance alarm-free performance. It is important that the sensors and/or cabling be attached per manufacturer specifications.

Types of Tests

- Unaided Climb Test

  The test consists of an individual (preferably a small individual) climbing the fence at various locations to verify that detection occurs. Attempts should be made near fence posts, especially corners/posts.

- Ladder Climb Test

  A ladder is placed against the fence. An individual climbs the ladder to the point of sensor activation. The ladder can be made more effective by adding padding to any point where the ladder may come in contact with the fence.

- Cutting Attack

  No actual cutting of the sensor wires or fence fabric should be performed.

- Jump Tests

  These tests cannot normally be conducted safely if a fence disturbance sensor is properly installed on a fence that is eight feet or more in height. However, adjacent structures used as platforms may permit an individual to jump over the fence/sensor wire, if personal safety can be ensured.

Test Guidelines

- All unaided climb tests should be conducted on several fence posts in at least two typical zones. Typically corner posts and heavy posts located at gates provide the highest probability of defeat by assisted and unassisted climbs.

- Zones that are substantially different (gates or different sensor configuration) should also be considered for testing.

- Areas that appear vulnerable to jumping should be tested to determine whether there is a vulnerability. Safety concerns should be addressed.

- If an individual sensor can be defeated, that same sensor should be tested again to determine whether the deficiency can be repeated. Several tests of the same sensor may be required to determine whether an adversary can reliably exploit the sensor deficiency.

- If an individual zone can be defeated, other zones should be tested using the same methods to determine the extent of the problem. The assessors should conduct several (three to five) more tests in different zones. If most of these tests indicate that the sensors can be reliably defeated, there likely is a systemic problem. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If the results are inconclusive, additional testing should be considered. Rarely would an assessor test more than 10 to 15 zones using the same methods.

- If the adversary has sufficient knowledge, time, and equipment, bridging or tunneling techniques can defeat all fence disturbance sensors. Such tests should only be conducted if a zone is particularly vulnerable (for example, due to barrier placement), or if patrol frequencies and direct visual observation (CCTV or from guard posts) are considered inadequate to reasonably ensure that such attempts are detected.

Checklist

Fence Disturbance Sensors

Exterior Perimeter IDS

Interview Items

Installation location: ____

____

Operational test frequency: ____

____

Operational test method: ____

____

Sensitivity test frequency: ____

____

Sensitivity test method: ____

____

Acceptance criteria for sensitivity test: ____

____

False alarm history/records: ____

____

Make/model: ____

____

Measures to prevent erosion: ____

____

Tamper switches (transmitter, receiver, junction boxes): ____________________________________

____

Tour/Visual Examination Items

Vegetation present? ____

____

Zone length OK? ____

____

Complements other sensors? ____

____

Overlap sufficient? ____

____

Data Collection Sheet
Fence Disturbance Sensors – Exterior Perimeter IDS

Test Method

	Zone Tested	Unaided Climb	Ladder Climb	Cutting	Jump
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

Comments:

Part 2

Interior Sensors

Part 2

Interior Sensors

Objective

The objective is to test the effectiveness of interior sensors in detecting adversary intrusion.

System Tested

System: IDS

Functional Element: Interior intrusion detection

Component(s): Interior sensors, transmission lines, alarm processing equipment, interfaces with CCTV and CAS operation, testing and maintenance of interior sensors

Scenario

The assessors should select several interior locations (material access areas, vaults, vital areas, or vault-type rooms) for testing, based on a number of factors: sensor types used, construction type, materials, configuration of the interior area, and operating history of the various sensors. At least one of each type of room or vault configuration and sensor should be tested.

The assessors should review building layouts and architectural drawings. They should also briefly tour the facility to familiarize themselves with typical protection system configurations and to identify potential weaknesses. The relationship between sensor application and the types of structural barriers in use should be noted. The detection capabilities of individual sensor types may vary depending upon the types of barriers used and the ability of these barriers to resist or delay penetration. Also, since some sensors respond to physical attacks on the barrier material, the detection technology employed (for example, acoustic, vibration, strain, or capacitance technologies) should be suited to the barrier material used.

In general, sensors consist of three generic types: motion (or area), barrier penetration, and proximity. Each type is subject to various physical and environmental limitations that must be considered when assessing suitability and operating performance. Limitations involve electromagnetic, radiological, acoustical, seismic, thermal, and optical effects, as well as the physical limitations imposed by equipment placement, room arrangement, and building materials used in walls, ceilings, floors, windows, doors, and penetrations (for example, ductwork and cable chases).

If possible, the assessors should observe alarm technicians or SPOs during the conduct of routine operational and sensitivity tests of selected sensors. The assessors should base their selection of the sensors to be tested on the number, type, configuration, and operational history of those sensors. During this portion of the test, assessors should observe calibration and maintenance procedures to determine whether they are consistent with DOE orders and approved SSSPs. In addition, observation of these tests may indicate the effectiveness of the test and maintenance program. Observations of facility-conducted tests are helpful in identifying the root causes of many noted deficiencies.

The assessors should conduct standard walk tests and tamper-indicating tests (provided no physical damage to the sensor will result) for each motion detection (area type) sensor tested. Barrier sensors (magnetic switches, glass sensors, and capacitance devices) and proximity sensors may require other tests as applicable and as identified in the manufacturer's instructions. The purpose of these tests is to determine whether each sensor type is functioning, whether it can detect attempted tampering, and whether it can detect its design basis target (intruder) or activity (for example, attempted barrier penetration using force or attack tools).

Within a single area, there may be several types of sensors that have different detection goals. For example, some barriers may have a penetration detection sensor, a volumetric area sensor for the interior, and a proximity or capacitance sensor to protect the actual item.

The assessors should monitor the alarm annunciation in the alarm stations. They should also observe the operation of any interfacing systems, such as CCTV displays and video recorders, to determine proper assessment.

The number of areas and sensor types to be tested depends on the available time, importance of the system in the overall protection program, and operating history. The following guidelines are intended to assist the assessor in selecting areas and sensors for testing:

- At least five protected interior areas (rooms/vaults/material access areas) should be tested. Priority should be given to those areas containing the most critical assets.

- At least one of each type of sensor should be tested, if possible, including motion sensors, penetration sensors, and proximity sensors, if used.

- If several tests of the same type of sensor are satisfactory, extensive testing of that sensor in different areas is unnecessary. However, if deficiencies are apparent, sufficient testing should be conducted to determine whether there is a systemic weakness.

- Tests should be conducted for selected areas where environmental concerns (noise, electromagnetic interference, temperature, and humidity changes) or physical obstructions are likely to degrade sensor performance.

Evaluation

If a detection system is to be effective, the sensors must detect intrusion, the alarm condition must be correctly assessed, and protective forces must be available for a timely response.

Assessing Sensor Performance

The primary objective in evaluating interior intrusion detection sensors is to determine whether they effectively detect penetration, intrusion, or proximity to protected devices or equipment. The following factors should also be considered:

- Do balanced magnetic switch (BMS) sensors initiate an alarm when exposed to an external magnetic field or when the switch is moved one inch from the magnet housing?

- Does the sensor layout allow adversaries to circumvent any sensor(s) because of alignment, obstructions, or environmental interference?

- Are there any temporary entry points or penetrations to barriers that could allow undetected intrusion?

Interpreting Results

The following guidelines are provided to assist the assessor in interpreting evaluation results.

- Many interior sensor systems employ redundant or layered protection schemes that rely on a combination of barrier, volumetric, and point protection systems. If any one of these is found to be deficient during testing, this finding should be evaluated in the context of the site-specific protection program objectives and the effectiveness of other complementary systems.

- In some cases, facility tests may indicate sensors are properly calibrated, but assessor tests may indicate that the sensors can be defeated or cannot reliably detect intrusion. In such cases, the assessor can reasonably conclude that there are deficiencies in the test and calibration procedures or in the quality assurance program, or both.

- When facility tests and calibrations are conducted properly, and the tests conducted by assessors indicate that sensors are performing according to specifications, the limitations of the facilities' test procedures must still be considered. Analysis should be conducted to verify that all modes of defeat and all physical and environmental factors have been considered in the facility-conducted tests.

- Sensor performance that does not appear to be in accordance with specifications may simply indicate sensor drift or an alignment problem. However, a systemic deficiency in sensor design, application, or maintenance might also be indicated. If the facility tests indicate that sensors are out of calibration, assessors should consider instructing the facility's technicians to test a representative sample of sensors to determine the extent of the problem.

Special Considerations

Some sensors are sensitive to the size of the intruder. The assessor should request the facility to provide a small person to conduct tests. Often, interior sensors may be located at ceiling height or in relatively inaccessible places (for example, in ductwork or cable chases). Ladders or other aids may be needed.

Related testing or activities, such as those for barriers, card access control systems, CCTVs, or line supervision or tamper indication, are typically conducted concurrently with sensor tests to minimize data-collection activities.

Responsibilities

Assessors: Select areas and sensors for testing. Direct tests and monitor alarm annunciation. Typically, one assessor will be located at the CAS/SAS and one assessor will be at the location of testing.

Facility: Conduct routine tests. Provide security technicians. Provide test devices and aids, as required. Provide SPOs for security and radios for two-way communication. Provide personnel to conduct testing at the direction of assessors or have the assessor conduct the test.

Internal Coordination

Testing should be coordinated to minimize the impact on facility operations and should not result in undue exposure of test personnel to radiological or other health hazards. Testing should also be scheduled to avoid conflicts with other tests involving other topic teams (for example, the protective force topic team).

Security Considerations

All normal security precautions should be taken. Normally, an SPO should be present to observe testing to ensure that there is no unauthorized access or activity at the protected location to be tested. In many cases, special security arrangements must be made before opening vaults or alarmed doors. These arrangements should be coordinated in advance to avoid delays during the testing.

Personnel Assignments

Test Director:

Facility Alarm System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- Alarm technician
- Testers
- SPOs to provide security during tests, as necessary.

Equipment:

- Radios
- Test devices (for example, infrared target simulator, glass-break detector, audio source).

Safety:

- Follow normal operating procedures.
- Complete a safety plan.
- Notify the CAS/SAS before testing is conducted.
- Station one assessor in the CAS/SAS.
- Coordinate with protective force personnel to prevent any undesired armed response to alarms.

Barrier Penetration Sensors

System Description:	BMS sensors, capacitance sensors, vibration sensors, and audio detectors; surface-mounted and coupled to a control device
Intruder Detection Capabilities:	Various, including physical proximity, forced opening, and physical attack using tools
Vulnerabilities:	Bypassing, tampering, substitution

Concerns

BMS Sensors:

- BMS sensors should have the switch mounted to a fixed surface, with the magnet mounted on the movable surface (door or window); capture or substitution of the magnet should be precluded.
- BMS sensors installed in areas posing a potential health hazard (for example, in radiation zones) should have self-checking test circuitry to eliminate the need for personnel to enter the hazardous area to check the devices.
- BMS sensors should always be installed on the protected side of the barrier to preclude tampering.
- BMS sensors should be mounted with tamper-resistant hardware to reduce the potential for surreptitious removal.

Capacitance Sensors:

- The capacitance sensor wire or "blanket" should not make contact with any grounded object or surface. Other grounded objects in the vicinity of the protected barrier, or in the presence of liquids on floors or other nearby surfaces, can drastically alter sensor capacitance.
- Control units for capacitance sensors should be located within the protected space to preclude tampering.

Vibration Sensors:

- Vibration sensors should be mounted within or on the protected inner surface of the protected barrier.
- Because there are several types of vibration sensors (piezoelectric, coaxial cable, wire tension, and others), the particular manufacturer's specifications must be consulted to determine sensor detection capabilities and weaknesses.

Audio Detectors:

- Audio detectors must be calibrated carefully to avoid nuisance alarms caused by common background noises (for example, machinery, vehicles, and other alarm signals).
- Audio glass-break detectors should be positioned to face the window(s) they protect.

Types of Tests

- BMS Sensors

  BMS sensors should be tested by opening the protected portal (door, hatch, or window) sufficiently to create an alarm. In general, an opening of one inch or less should generate an alarm. A second test should be conducted by placing a magnet near the BMS, which should also create an alarm since the switch's magnetic field is being disturbed.

- Capacitance Sensors

  Capacitance sensors are tested by approaching the protected surface and making physical contact. An alarm should occur with near contact or actual physical contact with the surface.

- Vibration and Audio Detectors

  Because various technologies are employed, the particular manufacturer's performance testing procedures should be followed, and any specified testing devices should be used.

Test Guidelines

- At least two typical zones should be tested.
- Any zones that have potential vulnerabilities because of sensor configuration, location, or environmental or structural concerns should be tested to reveal any exploitable deficiencies.

Checklist

Barrier Penetration Sensors

Interior Sensors

Interview Items

Installation location: ____

____

Operational test frequency: ____

____

Operational test method: ____

____

Sensitivity test frequency: ____

____

Sensitivity test method: ____

____

Acceptance criteria for sensitivity test: ____

____

False alarm history/records: ____

____

Make/model: ____

____

Tamper switches (transceivers, control units, junction boxes): ____

____

Tour/Visual Examination Items

Unprotected/vulnerable entry points present? ____

____

Sensor location adequate? ____

____

Sensor coverage adequate? ____

____

Sensor overlap sufficient? ____

____

Sensor compatible with structural materials? ____

____

Sensors compatible (if multiple sensors used)? ____

____

Obstructions or nuisance alarm sources present? ______________________________________

____

Control unit protected? ____

____

Data Collection Sheet
Barrier Penetration Sensors – Interior Sensors

Test Method

	Zone Tested	Functional Test	Sensor Type	Alarm Generation Method
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
Comments:				

Area Motion Sensors

System Description:	Ultrasonic, microwave, or passive infrared sensor; wall- or ceiling-mounted; coupled to control device; volumetric coverage pattern
Intruder Detection Capabilities:	Walking, slow walking, running, or crawling
Vulnerabilities:	Bypassing coverage pattern, target masking, extremely slow movement

Concerns

General:

- Optimum coverage requires direct line of sight. Obstructions such as columns, beams, storage racks or bins, furniture, or other large objects may prevent detection.
- Sensor transceivers and control units are subject to physical damage and tampering if they are not mounted to be inaccessible or are not covered by another sensor's detection pattern.
- Depending on the type used, sensors are susceptible to false alarms caused by moving objects (for example, fans), electromagnetic radiation, rapid temperature changes, air movement, seismic vibration, and background noise.
- Different sensor types have different coverage patterns (generally fan or wedge shaped). Proper overlap and coverage must be considered to ensure that an intruder cannot go over, around, or under the sensor's pattern of coverage.

Ultrasonic Sensors:

- Telephones, public address systems, alarm bells or sirens, and other loud sound sources can create nuisance alarms.
- Moving objects such as machinery, fans, venetian blinds or curtains, and wind-blown paper can create nuisance alarms.
- The sensor is less sensitive to a target moving across the detection zone than one moving directly toward or away from the detector.

Microwave Sensors:

- Moving objects such as machinery, fans, and venetian blinds or curtains can create nuisance alarms.
- The microwave detection beam can easily penetrate glass, wood, wallboard, and plastic (including water and drainpipes), creating false alarms from moving objects outside the protected space.
- Fluorescent light fixtures in the detection zone can create nuisance alarms.
- The sensor is less sensitive to a target moving across the detection zone, as opposed to moving toward or away from the sensor.
- The sensor is susceptible to masking (insider).

Infrared Sensors:

- Infrared will not penetrate any solid object, including glass. Movement in the area behind any objects in the detection pattern cannot be detected.
- Heat sources, such as radiators, electrical motors, and direct sunlight, can create nuisance alarms.
- Lights in the vicinity of the transceiver may attract insects, thereby creating nuisance alarms.
- The sensor is less sensitive to a target moving toward or away from the sensor than one moving across the detection zone.
- The sensor is susceptible to masking (i.e., by an insider).

Video Motion Detection Cameras:

- Detection effectiveness will decrease if minimum light levels are not maintained. Lighting is necessary even when the area is unoccupied.
- The lighting for a video motion detection system must be on an emergency power supply to be effective during a power failure.
- Some video motion cameras allow the CAS operator to define the detection zone. If the defined zone is too small, detection probability may be decreased.
- Video motion detection cameras frequently have difficulty detecting slow-moving objects.
- Video motion detection cameras require direct line-of-sight with no obstruction. If the detection capability is not verified when placed in secure mode, the video motion sensors can be rendered ineffective by blocking the field of view or covering the lens when the system is in access mode.
- The camera can be manipulated to mask intrusions.

Types of Tests

- Sensitivity Walk Test

  Walk tests are used to verify operability and sensitivity of the sensor. This test is performed by slowly walking (1 ft/sec) toward ultrasonic and microwave sensors until an alarm is received. For infrared sensors, the assessor walks slowly across the detection pattern, starting at a point outside the detection zone and proceeding inward until an alarm is received. This test should establish the far end of the sensor coverage pattern (see Evaluating Sensor Performance, page PSS-90).

- Crossing Walk Test

  This test verifies the ability of the sensor to detect motion along the least sensitive axis of the detection pattern. After the end of the sensor coverage pattern is determined from a sensitivity walk test, a crossing test should be performed by walking across the far end of an ultrasonic or microwave zone and by slowly walking toward the infrared sensor from various points outside the detection zone. Detection should occur before the tester enters the defined protected space or reaches the protected target/object.

- Avoidance Walk Test

  Based on the sensor coverage pattern (oval, wedge, or circle), the assessor should attempt to enter the target zone from a likely entry point (for example, from a doorway, a heating/ventilation/air-conditioning duct, or other weak point in the barrier system) or by walking around the sensor's zone of coverage. This test should verify adequate sensor coverage and overlap to detect movement in the protected space or movement of the target/object.

- Crawl Test

  A crawl test may be useful, depending on location of detector.

Test Guidelines

- Upon entering the room to be tested and prior to testing, the temperature and airflow inside the room should be allowed to normalize before testing begins. Observers should be requested to stand away from the area being tested.

- Testing should be conducted on at least two typical zones.

- Any zones that have potential vulnerabilities caused by obstructions or other sources of interference (for example, lighting, moving objects, noise, vibration, or heat sources) should be tested to determine whether there are exploitable deficiencies.

- Apparent weaknesses in zone coverage or sensor overlap should be tested to determine whether sensor coverage can be circumvented.

- Experience indicates that interior volumetric sensors are most vulnerable to a very slowly moving target entering the detection zone on the least sensitive axis (across the zones for ultrasonic and microwave sensors, and toward or away from infrared sensors).

- Many sensors have alarm indicator lights built into the sensor head. The assessors may observe these indicators to facilitate testing the coverage patterns or sensor sensitivity. However, the assessors should also verify that an alarm is received in the CAS/SAS to ensure that the alarm circuit is functional from sensor to annunciation point.

Checklist

Area Motion Sensors

Interior Sensors

Interview Items

Installation location: ____

____

Operational test frequency: ____

____

Operational test method: ____

____

Sensitivity test frequency: ____

____

Sensitivity test method: ____

____

Acceptance criteria for sensitivity test: ____

____

False alarm history/records: ____

____

Make/model: ____

____

Tamper switches (transceivers, control units, junction boxes): _________________________________

____

Tour/Visual Examination Items

Unprotected/vulnerable entry points present? ______________________________

____

Sensor location adequate? ______________________________

____

Sensor coverage adequate? ______________________________

____

Sensor overlap sufficient? ______________________________

____

Sensor compatible with structural materials? ______________________________

____

Sensors compatible (if multiple sensors used)? ______________________________

____

Obstructions or nuisance alarm sources present? ______________________________

____

Control unit protected? ______________________________

____

Data Collection Sheet
Area Motion Sensors – Interior Sensors

Test Method

	Zone Tested	Zone Number	Sensitivity Walk	Crossing Walk	Avoidance Walk	Crawl
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						

Comments:

Proximity Sensors

System Description:	Capacitance tuned circuit, point or proximity sensor, blanket or cable and contact configuration
Intruder Detection Capabilities:	Proximity/physical contact
Vulnerabilities:	Tampering with control unit

Concerns

- Some sensors experience "drift" in capacitance sensitivity over time and require regular sensitivity calibration.

- Sensors may be less effective at low temperatures and low sensitivity settings. Sensors are most reliable under temperature-controlled conditions.

- The capacitance sensor wire or blanket should not make contact with any grounded object or room surface. Other grounded objects close to the protected items, or liquids on the floor, may drastically alter the capacitance of the sensor.

- Control units for capacitance sensors should be located within the protected room or space to preclude tampering with sensitivity settings.

Types of Tests

- Capacitance sensors are tested by slowly approaching and physically touching the protected object with the hands. In an attempt to simulate an attempted compromise of this system, gloves should be worn to realistically desensitize the system. An alarm should be generated when in proximity to the object or upon physical contact.

Test Guidelines

- The person conducting the tests should remove all metal objects (radios, watch, coins, or a pocketknife) and should not wear steel-toed shoes. Gloves should be worn.

- Testing should be conducted on at least two typical zones.

- Any zones that have potential vulnerabilities such as unprotected metal objects near the protected target should be tested to identify any exploitable deficiencies.

Checklist

Proximity Sensors

Interior Sensors

Interview Items

Installation location: ____

____

Operational test frequency: ____

____

Operational test method: ____

____

Sensitivity test frequency: ____

____

Sensitivity test method: ____

____

Acceptance criteria for sensitivity test: ____

____

False alarm history/records: ____

____

Make/model: ____

____

Tamper switches (transceivers, control units, junction boxes): _______________________________

____

Tour/Visual Examination Items

Sensor location adequate? ____

____

Standing water present? ____

____

Grounded objects in proximity to protected object? ______________________________

____

Control unit protected? ____

____

Complements other sensors? ____

____

Data Collection Sheet
Proximity Sensors – Interior Sensors

Test Method

	Zone Tested	Zone Number	Approach and Touch
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Comments:

Part 3

Perimeter CCTV

Part 3

Perimeter CCTV

Objective

The objective is to test the effectiveness of perimeter CCTV systems for providing surveillance and assessment of alarms.

System Tested

System: Assessment system

Functional Element: Perimeter/exterior CCTV

Components: CCTV cameras, enclosures, towers, transmission lines, interface with IDS, and CAS/SAS switching and displays, testing and maintenance of exterior CCTV, lighting

Scenario

During an initial site tour, assessors should select various CCTV zones for testing, usually in conjunction with the exterior IDS test. Zone selection is based on a number of factors, including CCTV layout; fence line and IDS layout; perimeter lighting; visual obstructions such as buildings and manmade structures, terrain, and vegetation; and system operating history. The objective of the site tour is to identify potential problems created by irregular terrain (ditches, humps, dips), obstructions that block the view of a camera or create strong shadow effects, poor security lighting, poor camera placement or alignment, or improper association of camera zones with IDS zones.

The assessors should observe the facility's CCTV technicians and SPOs conducting routine operational and calibration tests of CCTV cameras and associated equipment, if possible. Cameras are identified for testing based on the number, type, configuration, and operating history. Test, calibration, and maintenance procedures are observed to determine whether they are consistent with DOE orders and approved SSSPs and whether they are an effective means of verifying proper system operation. Although it is desirable to observe these activities to determine system status and test and maintenance effectiveness, such tests should not be required if they are not part of the normally scheduled system checks.

The assessors should conduct individual camera testing during both daylight and darkness and, if practicable, at both sunset and sunrise. This testing is important to verify that the cameras function properly throughout the full range of lighting conditions. Testing generally consists of run tests across the isolation zone between the outer and inner perimeter fence lines to determine whether the automatic camera call-up, following IDS activation, is rapid enough to allow observation of an intruder within the camera field of view. In addition, testing is conducted at the far end of the field of view to verify that camera lens selection provides a discernable image at the maximum viewing distance. Other tests are conducted where features of terrain, obstruction, or lighting indicate that CCTV coverage may not be effective. The purpose of these tests is to determine whether an adversary could cross the perimeter isolation zone, or remain in that zone, without being observed.

The assessors should monitor the camera displays in the CAS and/or SAS, and observe operation of supporting subsystems, such as camera switching, sequencing, video recording, pan-tilt-zoom (PTZ) control, and date/time

generation, if used. The assessors should also observe the interfacing of systems, including automatic call-up of CCTV upon IDS activation, CAS/SAS operator actions, and control and direction of response forces based on CCTV assessment of adversary actions.

The number of camera zones selected for testing depends on the time available, the importance of CCTV in the overall assessment system, and the number of potential deficiencies identified during the site tour. The following guidelines are intended to assist the assessor in selecting zones for testing:

- Normally, a minimum of two camera zones should be tested in conjunction with the perimeter IDS test. If zone camera configurations vary (for example, cameras facing one another versus cameras that follow in sequence) or if automatic camera call-up differs because of changes in the IDS sensors used, a representative sample of each configuration type should be tested.

- If a variety of cameras and camera lenses are employed, a representative sample should be tested.

- If PTZ cameras are used for perimeter surveillance, at least one of these cameras should be checked, particularly if it is the type that automatically shifts to a preset field of view upon IDS activation. PTZ cameras should not be the primary means of assessment in a perimeter intrusion detection and assessment system.

- If special application cameras are used (for example, very low light level or infrared), at least one should be tested.

- Tests should be conducted for selected zones in which deficiencies are anticipated due to terrain, vegetation, obstructions, or lighting conditions.

- If the initial tests do not indicate problems and the camera scenes displayed at the CAS/SAS appear to be generally clear and uniform, the assessors need not test numerous cameras. However, if deficiencies are apparent, the assessors should collect sufficient data to determine whether the weakness is an isolated problem or a systemic deficiency.

- Tests should be conducted to evaluate speed of camera call-up and assess whether any vulnerabilities exist as a result.

Evaluation

The purpose of a CCTV assessment system is to support the intrusion detection and response functions by promptly and accurately assessing alarms (to include verification of nuisance and false alarms), determine adversary actions, and direct protective force response. The principal factor in evaluating the CCTV system is whether it effectively and reliably provides prompt and complete observation of the perimeter isolation zone and particularly the area adjacent to the inner perimeter fence line in any zone from which an alarm is received. Other factors to consider in the evaluation are:

- Is the CCTV system the sole or primary means of assessment and observation, or do SPOs observe the perimeter? System requirements (such as automatic camera call-up) vary depending upon the degree of reliance on CCTV.

- Does the camera layout provide complete coverage of the isolation zone or do gaps occur that could be exploited by an adversary?

- Do terrain irregularities, visual obstructions, shadows, or lighting deficiencies create exploitable weaknesses in the camera coverage?

- Does the CAS/SAS display function of the CCTV system adequately support the assessment requirement in terms of speed of camera call-up, resolution, size of monitor display, and video recording, as applicable to system configuration and the availability of other assessment aids?

- Is the CCTV equipment capable of performing properly in all light conditions, day or night?

- Is the CCTV equipment capable of assessing alarms during a loss of lighting as a result of loss of power?

- Are the monitor displays (if any) in security towers or other guard posts functional and effective for their intended purpose?

- Are environmental concerns adequately addressed for all expected climatic conditions in terms of environmental enclosures, heaters, blowers, wipers, and other such devices?

Interpreting Results

The following guidelines are provided to assist assessors in interpreting results in the context of overall system performance:

- As with other security elements, a perimeter CCTV system is only as strong as its weakest link. Tests that indicate that an adversary can cross a camera zone without observation, following IDS activation, are evidence that the CCTV assessment system is not fully reliable. The significance of this finding must be analyzed in the context of the site-specific protection objectives and the effectiveness of other assessment aids.

- In some cases, facility tests indicate that visual obstructions, lighting deficiencies, or other weaknesses exist in individual camera zones. However, the capability to assess perimeter alarms remains because of partial coverage from an adjacent camera or from direct visual observation. In such cases, the deficiencies are of lesser concern because other assessment aids provide compensation. However, these deficiencies may indicate problems in system design or in the test and maintenance program. Testing and maintenance deficiencies may be attributed to inadequate maintenance procedures, insufficient attention to reported problems, or incomplete procedures for reporting CCTV failure or degradation.

- Facility tests that indicate that cameras are properly calibrated and aligned, in conjunction with tests conducted by assessors that indicate an intruder can be effectively observed, are evidence that tested portions of the system are operational and maintenance procedures are effective. However, facility tests do not ensure that all modes of defeat have been assessed or that all weather and lighting conditions have been evaluated to maximally stress the system.

- Facility tests that indicate that individual cameras are not operating in accordance with the manufacturer's specifications may simply be an indicator of isolated equipment degradation. However, such deficiencies may be evidence of a system-wide weakness in the maintenance program or a failure of system components due to age. Most camera image tubes have a predictable useful life, after which rapid degradation and failure can be expected. If all of the cameras in the system were installed at the same time, camera failures likely will occur in rapid succession throughout the system. Life cycle planning for the maintenance and replacement of equipment is required to avoid this issue and should be documented in maintenance procedures.

Special Considerations

Some sites employ specialized camera equipment, such as video motion detection systems or very low-light-level cameras, that have special test requirements. In such cases, assessors should be sure to familiarize themselves with the manufacturer's instructions for operation, test, and maintenance of the equipment.

Special attention should be paid to nighttime lighting conditions, including shadowed areas and the effects of transient lighting changes due to vehicle headlights and opening of doors. To increase the efficiency of the data-gathering effort, CCTV testing should be integrated with related assessment activities, such as barrier examinations, IDS testing, and checks of tamper and line supervision alarms.

Responsibilities

Assessors: Select cameras for testing. Direct testing and monitor video displays and recording. Typically one assessor will be stationed at the CAS and at least one at the perimeter.

Facility: Conduct routine testing. Provide technicians and test devices, as necessary. Provide radios for two-way communications. Provide security compensatory measures, as required. Provide personnel (normally an SPO) to conduct zone testing at the direction of assessors.

Internal Coordination

Testing should be scheduled to avoid conflicts with exercises or activities involving other topic teams (primarily the protective force topic team). Daytime testing is typically conducted concurrently with the perimeter IDS testing.

Security Considerations

All normal security considerations should be observed. Normally, an SPO must monitor (directly or using CCTV) test activity to ensure that no unauthorized personnel enter the Protected Area.

Personnel Assignments

Test Director:

Facility CCTV System Point of Contact:

Facility Protective Force Representative:

Assessment Team Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- CCTV technicians
- Tester.

Equipment:

- Radio
- Contrasting clothing for nighttime tests.

Safety:

- Follow normal operating procedures.
- Complete a safety plan.
- Notify the CAS/SAS before testing is conducted.
- Station one assessor in the CAS.
- Coordinate prevention of any armed response in the area of test personnel.

Perimeter CCTV Testing
and Long Range Camera/Tracking Systems

System Description:	Fixed and PTZ cameras, usually with low-light capability, mounted on pole, tower, or wall; coaxial, fiber optic, cable or microwave transmission; associated switching, display, and recording equipment
Capabilities:	Perimeter surveillance and intrusion assessment with ability to discriminate human intruders from animals or other causes of false or nuisance alarms from the perimeter IDS
Vulnerabilities:	Extreme weather (ice, snow, fog, rain, wind), inadequate security lighting, improper alignment or overlap, and visual obstructions or shadows caused by structures or uneven terrain

Concerns

- Cameras and associated supporting systems (switches, monitors, and recorders) are complex devices requiring extensive maintenance and calibration. Certain components are subject to predictable failure due to age, and may result in a system-wide outage.

- CCTV capability may be seriously degraded by weather extremes (ice, fog, snow, rain, wind-blown dust). Where extremes are prevalent, environmental housings (blowers, heaters, wipers) should be present and in good working condition.

- If CCTV towers, poles, or wall mounts are not rigid, the cameras are subject to wind-induced vibration, which can cause loss of video assessment capability.

- For outdoor application, cameras should have a broad dynamic range to allow for effective operation during daylight and darkness. Light-limiting and auto-iris capabilities should be provided to compensate for varying background light levels and to minimize “bloom” from bright light sources (perimeter lighting, vehicle headlights).

- Visual obstructions (buildings, vegetation, towers, fences, structures, or terrain irregularities) can block camera fields of view, creating the potential for intruders to hide or to cross the isolation zone without being observed. The shadows from such obstructions can also interfere with effective observation.

- If camera placement or alignment is improper, there may be “holes” in the CCTV coverage that permit an unobserved intruder to cross the isolation zone. Additionally, if the field of view of the camera is too long for the camera lens, an intruder at the extreme end of the field of view may not be adequately observed. (Note: Industry requires that the postulated adversary occupy at least five vertical scan lines when standing at the far end of the camera’s field of view.)

- If cameras are located outside of Protected Area boundaries (to provide better coverage within IDS zones), they may be more vulnerable to tampering.

- Automatic camera call-up on the alarm monitor at the CAS/SAS, upon activation of an IDS sensor (if employed), should be sufficiently rapid to observe the intruder before he/she crosses the isolation zone and reaches the inner perimeter fence. Alternatively, the video-recording system (digital or laser disk) should be capable of recording and playing back the camera scene showing the intruder crossing the isolation zone.

- PTZ cameras should have limit switches to preclude their facing directly into bright light sources. Also, if they are called up by IDS activation, they should be programmed to automatically position themselves to view the area from which the alarm was received.

Types of Tests

- Functional Test

  A functional test of each camera should be performed from the CAS/SAS by calling up each camera scene to verify that cameras are operating and that a clear image is received. If multiple monitors are used for continuous display (for example, nine-inch sequenced monitors), assessors should verify their function and sequencing. Assessors should also check all PTZ functions for proper operation and examine video-recording systems.

- Field-of-View Test

  In conjunction with the perimeter IDS test, assessors should conduct field-of-view tests if the far point of the camera field of view appears to be excessively long (that is, a clear image of an intruder cannot be seen at the far end of the camera's field of view). To conduct this test, a person should be positioned at the far end of the field of view and should slowly walk across the isolation zone. This test should also verify that the inner perimeter fence line is within the field of view of each camera that observes the isolation zone.

- Obstruction Test

  A test should be conducted when an identified obstruction or shadow may preclude effective observation. This test is conducted by having a person run to and hide behind the obstruction or in the shadowed area.

- Camouflage Test

  A test should be conducted to see whether a color or style of clothing is not visible to the camera.

- Speed of Response Test

  At a narrow point in the isolation zone, a person should run through the IDS sensor zone to the inner perimeter fence line. This test is used to verify that automatic camera call-up and/or video recording is sufficiently rapid to allow observation of the intruder before he/she can leave the isolation zone and the camera's field of view.

Test Guidelines

- All of the foregoing tests should be conducted during daylight and at night to ensure that lighting is adequate and cameras can function properly in low-light conditions. Additionally, the functional test should be conducted at sunrise or sunset to verify that positioning the camera directly toward the sun doesn't degrade camera functions.

- Obstruction tests should be conducted whenever functional tests indicate that the assessment capability in a camera zone is significantly degraded by the obstruction.

- If a significant number of camera zones (more than 10 percent) exhibit degraded picture quality, maintenance records should be reviewed to determine whether useful camera life limits might have been reached due to not replacing camera image tubes.

Checklist

Perimeter CCTV Testing
and Long Range Camera/Tracking Systems

Exterior Perimeter

Interview Items

Installation location: ____

____

Operational test frequency: ____

____

Operational test method: ____

____

Calibration test frequency: ____

____

Calibration test method: ____

____

Acceptance criteria for calibration test: ____

____

Make/model: ____

____

Environmental protection equipment: ____

____

Special equipment (recorders, PTZ cameras): ____

____

Maintenance history/records: ____

____

Mounting method (tower, pole, wall): ____

____

Tamper switches (transmitter, receiver, junction boxes): ____

____

Tour/Visual Examination Items

Obstructions present? ____

____

Shadows present? ____

____

Terrain level? ____

____

Zone length OK? ____

____

PTZ cameras, other cameras? ____

____

Overlap sufficient? ____

____

Mounting towers/poles rigid? ____

____

Lighting adequate? ____

____

Environmental housings adequate? ____

____

Data Collection Sheet
Exterior Perimeter CCTV System

Test Method

	Zone Tested	Functional Test	Field of View Test	Obstruction Test	Speed of Response Test
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

Comments:

Part 4

Interior CCTV

Part 4

Interior CCTV

Objective

The objective is to test the effectiveness of interior CCTV systems in providing surveillance and assessment of intruder movement and actions.

(Note: CCTV cameras that are physically located outside but cover the exteriors of portals or emergency exits are included within the scope of this performance test.)

System Tested

System:	Assessment system
Functional Element:	Interior CCTV
Components:	CCTV cameras, enclosures, mounts, transmission lines, interface with the IDS and the CAS/SAS, switching and displays, and testing and maintenance of the interior CCTV

Scenario

The assessors should select various CCTV zones for testing, usually in conjunction with interior IDS tests, during an initial facility tour. Zone selection is based on a number of factors, including CCTV layout, IDS configuration, interior lighting, and operating history of the cameras. The assessors should review building layouts, architectural drawings, and briefly tour the facility to familiarize themselves with the location of protected spaces in relation to camera coverage. This tour should reveal potential problems created by camera placement, visual obstructions, poor lighting, and improper camera alignment.

The assessors should observe, whenever possible, the facility's CCTV technicians and SPOs as they conduct routine operational and calibration tests of CCTV cameras and associated equipment. Cameras are selected for testing according to the number, type, configuration, and operating/maintenance history of the units in the system. Test, calibration, and maintenance procedures are observed to determine whether they are consistent with DOE orders and approved SSSP requirements, and whether they are an effective means of verifying proper system operation.

The assessors should conduct individual camera testing during various lighting conditions, if practical, to verify that cameras function properly throughout the full range of light conditions. Testing generally consists of walk tests within various camera zones to determine whether coverage allows observation of an intruder within the camera's field of view. In addition, testing should be conducted at the most distant end of the field of view to verify that the camera lens provides a discernable image at the maximum viewing distance. Other tests are conducted where camera placement, alignment, obstructions, or lighting conditions indicate that CCTV coverage may not be effective. The purpose of these tests is to determine whether an adversary could enter, exit, or remain within a protected space without being observed.

Assessors should monitor the camera displays in the CAS and SAS to observe the operation of supporting subsystems, such as camera switching, sequencing, video recording, PTZ control, and date/time generation. The

assessors should also observe the interfacing of systems, including automatic call-up of CCTV upon IDS activation, CAS/SAS operator actions, and control and direction of response forces based on CCTV assessment of adversary actions.

The number of camera zones selected for testing depends on the time available, the importance of CCTV in the overall assessment system, and the number of potential deficiencies identified during the site tour. The following guidelines are intended to assist the assessor in selecting zones for testing:

- A minimum of two camera zones should be tested, normally in conjunction with the interior IDS test. If camera configurations vary or if automatic camera call-up differs because of changes in the IDS sensors used, a representative sample of each type of configuration should be tested.
- If a variety of camera lenses and focal lengths are employed, a representative sample should be tested.
- If interior PTZ cameras are used, assessors should check at least one, particularly if it is one that automatically shifts to a preset field of view upon IDS activation.
- If special-application cameras are used (for example, very-low-light-level, video motion detection, or infrared), at least one should be tested.
- Assessors should conduct tests on cameras for which deficiencies are anticipated because of configuration, alignment, obstructions, or light conditions.
- If initial tests do not indicate problems, and the camera scenes displayed at the CAS/SAS appear to be generally clear and uniform, the assessors need not test numerous cameras. However, if deficiencies are apparent, the assessors should collect sufficient data to determine whether the weakness is isolated or systemic.
- Procedures should be in place to assure that no obstructions can be placed in the “assessment area.”

Evaluation

The purpose of a CCTV assessment system is to support the intrusion detection and response functions by promptly and accurately assessing alarms (to include verifying nuisance and false alarms), determine adversary actions, and direct protective force response.

Assessing System Effectiveness

The principal objective in evaluating the CCTV system is to determine whether it effectively and reliably provides prompt and adequate observation of the protected space and the principal entry points. The following points should be considered in the evaluation:

- Is the CCTV system the sole or primary means of assessment and observation, or do SPOs provide visual observation of the area? System requirements (such as automatic camera call-up) vary, depending on the degree of reliance on CCTV.
- Does the camera layout provide complete coverage or are there gaps that could be exploited by an adversary?

- Are there visual obstructions and procedures or lighting deficiencies that create exploitable weaknesses in the camera coverage?

- Does the CAS/SAS display function of the CCTV system adequately support the assessment requirement? Aspects to consider include the speed with which cameras are called up, resolution and size of monitor displays, and video recording.

- Is the CCTV equipment capable of performing properly in all light conditions, day or night?

- Are the monitor displays (if any) at guard posts functional and effective for their intended purposes?

- Are all essential cameras in the system functional (or compensatory measures in place)?

Interpreting Results

The following guidelines are provided to assist assessors in interpreting results in the context of overall system performance:

- Testing that indicates that an adversary can cross a camera zone unobserved following IDS activation is evidence that the CCTV assessment system is not fully reliable. The significance of this deficiency must be analyzed in the context of the site-specific protection objectives and the effectiveness of other assessment aids.

- In some cases, facility testing indicates that there are visual obstructions, lighting deficiencies, or other weaknesses in individual camera zones. However, the capability to assess IDS alarms remains because of partial coverage from an adjacent camera or direct visual observation. Although these weaknesses are less serious because of these compensatory measures, they may indicate problems in system design or the test and maintenance program. Test and maintenance deficiencies may be attributed to inadequate maintenance procedures, insufficient attention to reported problems, or incomplete procedures for reporting CCTV failure or degradation.

- Facility testing that indicates cameras are properly calibrated and aligned, in conjunction with assessment team testing that indicates that an intruder can be effectively observed, is evidence that tested portions of the system are operational and that maintenance procedures are effective. However, such tests do not ensure that all modes of defeat have been assessed or that all conditions have been evaluated.

- Facility testing that indicates that individual cameras are not operating in accordance with the manufacturer's specifications may simply be an isolated instance of equipment degradation. However, such deficiencies may also be evidence of a system-wide problem regarding the maintenance program or component aging. Most camera image tubes have a predictable useful life, after which rapid degradation followed by failure can be expected. If all of the cameras in the system were installed at the same time, camera failures will likely occur in rapid succession throughout the system. To avoid this multiple failure problem, life cycle planning for the maintenance and replacement of equipment is required, the written details of which should be included in the facility maintenance procedures.

Special Considerations

Some sites employ specialized camera equipment, such as video motion detection systems or very-low-light-level cameras, which have special test requirements. For such equipment, assessors should familiarize themselves with the manufacturer's instructions.

Special attention should be paid to nighttime and after-hours lighting conditions, including shadowed areas and the effects of transient lighting changes due to vehicle headlights, opening of doors, or other light sources.

Has the system been reviewed for classification? How is the video protected from unauthorized access?

To increase the efficiency of the data-gathering effort, CCTV testing should be integrated with related assessment activities, such as barrier examinations, IDS tests, and checks of tamper and line supervision alarms.

Responsibilities

Assessors: Select cameras for testing. Direct testing and monitor video displays and recording. Typically, one assessor will be stationed at the CAS and at least one with the test team.

Facility: Conduct routine testing. Provide technicians and test devices, as necessary. Provide radios for two-way communications. Provide for security compensatory measures, as required. Provide personnel (normally an SPO) to conduct zone tests at the direction of the assessors.

Internal Coordination

Testing should be scheduled to avoid conflicts with the activities and performance tests conducted by other topic teams (primarily the protective force topic team). Testing typically should be conducted concurrently with interior IDS tests.

Security Considerations

All normal security considerations should be observed. Normally, an SPO must monitor (directly or via CCTV) test activity to ensure that no unauthorized personnel enter protected spaces.

Personnel Assignments

Test Director:

Facility CCTV System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- CCTV technicians
- Tester.

Equipment:

- Radio.

Safety:

- Follow normal operating procedures.
- Complete a safety plan.
- Notify the CAS/SAS before conducting any test.
- Station one assessor in the CAS.
- Coordinate with protective force personnel to prevent any undesired armed response.

Interior CCTV Testing

System Description:	Fixed and PTZ cameras, wall or ceiling bracket-mounted; coaxial cable or fiber optic transmission; associated switching, display, and recording equipment
Capabilities:	Interior surveillance and intrusion assessment, with ability to differentiate between humans and animals, or other causes of false or nuisance alarms generated by the interior IDS
Vulnerabilities:	Inadequate lighting, improper alignment or overlap, and visual obstructions

Concerns

- Cameras and associated supporting systems (switches, monitors, and recorders) are complex devices requiring extensive maintenance and calibration. Certain components are subject to predictable failure as they age. Failure because of aging may be a system-wide occurrence if several cameras were installed at the same time.

- Visual obstructions can block camera fields of view, creating the potential for intruders to hide or to cross the camera zone without being observed.

- Camera image tube and video monitor burn-in can result from constant focus on a high-contrast background (extreme light to dark ratio), which degrades camera and video monitor performance.

- If camera placement or alignment is improper, there may be holes in the CCTV coverage that could permit unobserved intruder access. Additionally, if the camera's field of view is too long for the camera lens, an intruder at the extreme end of the field of view may not be adequately observed.

- Automatic camera call-up on the alarm monitor at the CAS/SAS upon activation of an IDS sensor (if employed) should be rapid enough (no more than two seconds) to observe the intruder before he/she crosses the camera's field of view. Alternatively, the video recording system (digital or laser disk) should be capable of recording and playing back the camera scene showing the intruder crossing the camera zone.

- PTZ cameras should have limit switches so they will not face directly into bright light sources. Also, if PTZ cameras are automatically called up by IDS activation, they should be programmed to automatically position themselves to view the area from which the alarm was received.

Types of Tests

- Functional Test

  A functional test of each camera should be performed from the CAS/SAS by calling up each camera scene to verify that all cameras are operating and that a clear image is received. If multiple monitors are used for continuous display, their function and sequencing (if employed) should be verified. Any PTZ functions should also be checked for proper operation, as should video-recording systems.

- Field-of-View Test

  In conjunction with the interior IDS test, field-of-view testing should be conducted if the far point of the camera's field of view appears to be excessively long (that is, a discernible image of an intruder cannot be obtained at the far end of the camera's field of view). To conduct this test, a person should be positioned at the far end of the field of view and should walk slowly across that field of view. In general, this test should also verify that critical access portals are within the camera's field of view.

- Obstruction Test

  A test should be conducted whenever an obstruction and/or lighting conditions could preclude effective observation. This test is conducted by having a person hide behind the obstruction or in a darkened area.

- Speed of Response Test

  To test for speed of camera response when automatic call-up of a camera upon IDS activation is employed, a person should activate an interior sensor and then attempt to rapidly exit the area covered by the camera. This test is used to verify that automatic camera call-up and/or video recording is rapid enough to allow observation before the intruder can leave the camera's field of view.

Test Guidelines

- All of the foregoing tests should be conducted under various conditions to ensure that the cameras can function in all light conditions, as applicable.
- At a minimum, test at least two camera zones, if possible.
- Conduct obstruction tests whenever functional testing indicates that the assessment capability in a camera zone is significantly degraded by an obstruction.
- If a significant number of camera zones (more than 10 percent) exhibit degraded picture quality, maintenance records should be reviewed to determine whether useful camera life limits have been exceeded because camera image tubes have not been replaced.

Checklist

Interior CCTV System

Interview Items

Installation location: ____

____

Operational test frequency: ____

____

Operational test method: ____

____

Calibration test frequency: ____

____

Calibration test method: ____

____

Acceptance criteria for calibration test: ____

____

Make/model: ____

____

Camera mounting hardware: ____

____

Special equipment (recorders, low-light-level or PTZ cameras): ____

____

Maintenance history/records: ____

____

Tamper switches (transmitter, receiver, junction boxes): ____

____

Tour/Visual Examination Items

Obstructions present? ____

____

Zone length OK? ____

____

PTZ cameras, other cameras? ____

____

Overlap sufficient? ____

____

Mounting adequate? ____

____

Lighting adequate? ____

____

Data Collection Sheet
Video – Interior CCTV

Test Method

	Zone Tested	Functional Test	Field of View Test	Obstruction Test	Speed of Response Test
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

Comments:

Part 5

Alarm Processing and Display

Part 5

Alarm Processing and Display

Objective

The objective is to test the effectiveness of alarm processing, annunciation, and display at alarm stations.

System Tested

System: Alarm station functions

Functional Element: Alarm processing and display equipment

Components: Alarm monitors and displays, alarm printers, recording devices, annunciator panels, related equipment controls, switchers, and equipment testing and maintenance

Scenario

Alarm processing and display equipment encompasses all of the annunciation, monitoring, and display equipment and devices employed at the CAS/SAS. This equipment is used to monitor and record the activity associated with all other active subsystems in the security system including: CCTV, IDSs, tamper and line supervision alarms, emergency power supplies, communications equipment, access controls, and search equipment.

Since alarm processing and display functions are directly related to the operation of other subsystems, a specific test of such functions is not conducted. Rather, the assessors note the effectiveness of displays and annunciations at the CAS/SAS in the course of conducting other tests on IDS, access controls, and other systems. The alarm processing and display functions to be tested depend upon the types of security subsystems in use and the types of annunciation/display equipment used at the CAS and SAS. The assessors should review building layouts and security system drawings and tour the facility to familiarize themselves with systems configuration and operations so as to effectively evaluate systems annunciation and display capabilities.

While conducting individual subsystems tests, the assessors note the effectiveness of annunciation and display of alarms, camera scenes, or status indication for the following subsystems or components:

- Interior and exterior IDS alarms
- Line supervision and tamper-indication alarms
- CCTV display monitors and recording devices
- Biometric and/or card access controls
- Search equipment (special nuclear material detectors, metal detectors), if appropriate
- Power supplies
- Activated barriers (smoke, foam)
- Remotely operated vehicle barriers and gates.

Any components used to maintain a historical record of alarms, displays, or status indication are also to be reviewed. These components include alarm logs maintained by computer memory or on storage media (computer tapes or disks), computer printouts, chart recorders, or video recordings, as appropriate.

Assessors must also verify that the SAS is properly equipped and operated to serve as a completely functional backup to the CAS (where required). The SAS must be capable of performing all required alarm response functions. At some facilities, an alarm condition is annunciated in the SAS only if the CAS operator fails to acknowledge it within a prescribed period. Assessors may elect to verify the operation of such an alarm annunciation capability.

The following guidelines are intended to assist the assessor in selecting items of equipment for testing:

- Evaluate at least one example of each type of annunciation device, display, status indicator, control device, or recording/logging device, if possible.
- Verify that the system functions under emergency power supply conditions and shows no degradation of alarm processing and display.
- Evaluate CCTV system displays and video-recording capability under conditions of both daylight and darkness.

Evaluation

The purpose of alarm processing and display functions is to ensure the capability of the CAS/SAS to control, monitor, and respond to all components of the facility security systems. These functions directly support the requirements to promptly and accurately assess alarms, provide personnel access controls, determine adversary actions, and direct protective force response.

Assessing System Effectiveness

The principal objective in evaluating the alarm processing and display system is to determine whether it effectively and reliably provides prompt and adequate control and monitoring of critical security systems. Other points to consider in the evaluation are:

- Do all alarms provide clear audible and visual annunciation/display?
- Are there provisions to call the CAS/SAS operator’s attention to an alarm-associated camera display?
- Does the monitoring equipment provide for straightforward and easy acknowledgment of all alarms?
- Is the status of all power supplies (normal alternating current, batteries, and generators) clearly indicated at all times?
- Are video displays and recordings clear and available at the CAS and SAS?
- Are line-supervision and tamper-indication alarms clearly displayed and distinguished from other alarm conditions?
- Are alarm processing and display equipment adequately protected against tampering or physical attack?
- Are scheduled testing and maintenance performed on all alarm processing and display equipment?
- Are invalid or unauthorized keycard (or biometric) access attempts promptly and clearly annunciated?

- Does the system provide a historical log of all keycard or biometric access transactions?
- Are controls for security lighting and emergency power available at the CAS and SAS?
- Are there provisions to ensure that the SAS operator is aware of changes in the status of IDSs (for example, from secure to access)?
- Are records of false and nuisance alarms maintained by the system?

Interpreting Results

The following guidelines are provided to assist assessors in interpreting results in the context of overall system performance:

- The types of alarm processing and display systems in use at DOE contractor facilities vary considerably because of differences in the ages of the systems, the degree of computerization employed, and the size and sophistication of the total site security system. Therefore, considerable judgment must be used in evaluating system effectiveness. The key factors considered are whether displays are prompt, clearly annunciated, and understandable. Human factor concerns are important in determining whether an operator can effectively interact with the system to assess and respond to annunciations and displays.
- Another critical factor in evaluating system adequacy is the ability of the SAS to function as an effective backup to the CAS. In determining this adequacy, the assessor should assess whether the SAS can function in a standalone mode to completely and effectively monitor, control, and respond to all critical security system functional elements.

Special Considerations

For those sites that use computer-based alarm processing and display systems, it may be necessary to interview the systems analyst or programmer responsible for system software. Some system anomalies may be due to hardware defects or may be the result of programming errors. Another problem relative to computer-based alarm systems is the control of software and its protection against the insider threat. This problem is such that it requires management support and oversight at the highest level possible.

For CCTV system displays and recorders, testing under conditions of both daylight and darkness is required to evaluate system effectiveness.

In the interest of efficiency in data gathering, system testing should be conducted in conjunction with testing scheduled for CCTV, IDSs, access controls, emergency power supplies, and other subsystems of the site security system.

Responsibilities

Assessors: Select systems for testing. Direct testing and monitor annunciation, displays, and recordings. Typically, one assessor will be stationed at the CAS and at least one with the test team.

Facility: Conduct routine tests. Provide technicians and test devices as necessary. Provide radios for two-way communication. Provide security compensatory measures, as required.

Internal Coordination

- Conduct testing concurrently with and as an aspect of other system tests.
- Observe all normal security considerations.

Personnel Assignments

Test Director:

Facility System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- Technicians
- Tester
- Systems analyst or programmer.

Equipment:

- Radio.

Safety:

- Follow normal operation procedures.
- Complete a safety plan.
- Notify the CAS/SAS before conducting testing.
- Station one assessor in the CAS or SAS.
- Test personnel should arrange to prevent any undesired armed protective force response.

Alarm Processing and Display Equipment

General Characteristics:	CAS/SAS alarm consoles, alarm annunciators and displays, system status indicators, CCTV monitors and recorders, personnel and vehicle access controls, lighting and emergency power controls, and various support equipment
Capabilities:	Security system monitoring, control, assessment, and historical recording, as appropriate; redundant command and control capabilities at CAS and SAS
Vulnerabilities:	Poor human-machine interface, excessive numbers or differing types of displays, inadequate redundancy between CAS and SAS

Concerns

- High numbers of nuisance/false alarms may degrade operator response to genuine alarm conditions.

- Failures of the system to adequately identify alarm type and specific location may degrade response. This is usually most evident in systems that do not clearly differentiate between tamper-indication or line-supervision alarms, or when multiple sensors are monitored by a single circuit (for example, alarms in series).

- In older systems that do not use a computer-based integrated alarm processing system, a variety of different alarm panels and status indicators may be employed. This can cause inefficiency and confusion in assessing and acknowledging alarms because the operator must respond to several standalone annunciators.

- In older computer-based systems, problems may arise from the computer's lack of speed or from inadequate alarm prioritization. In those cases, the system is unable to expeditiously and effectively sort significant quantities of simultaneous, or near simultaneous, alarm information and the system becomes bogged down resulting in slower alarm processing, storing alarm information without prioritization, or (in the worst case) a system crash. If such conditions were to occur, the ability of the operator to provide timely detection/assessment information to the protective force would be severely degraded, as would the protective force's ability to respond rapidly.

- For computer-based systems, problems may also arise as new or additional sensors or access control devices (ACDs) are added over time. Each time the system configuration changes, software programming changes are required in the system. Unless software modifications and system configuration are carefully controlled, program errors may be generated.

Types of Tests

- Function Test

  Assessors should perform a functional test of each type of alarm annunciator, status indicator, or control device in conjunction with each subsystem test (for example, CCTV, IDS, access control, emergency power test). The purpose of each test is to verify proper system function and to determine whether alarm annunciation, acknowledgement, and command/control are clear and straightforward. Promptness of alarm display following field device activation should be checked concurrently.

- Historical Record Test

  Evaluate any historical records maintained by the system (for example, alarm logs, access control transaction histories, and video recordings) for completeness and accuracy. False and nuisance alarm rates may also be assessed by reviewing these records.

- SAS Test

  Test a representative number of alarm annunciations and command/control functions at the SAS to determine whether the SAS provides adequate backup to the CAS. As part of this testing, assessors should verify that the SAS is capable of knowing about any command actions taken by the CAS that change alarm points or ACDs from the secure mode to the access mode or that enable/disable security devices.

Test Guidelines

- Conduct testing of alarm processing and display in conjunction with other system tests.
- Test CCTV displays and recording capabilities during both daylight and darkness.
- At a minimum, test at least one of each type of alarm annunciation, recording device, and command/control function.
- Conduct a separate limited-scope performance test of the SAS to verify its adequacy as a backup to the CAS.

Checklist

Alarm Processing and Display Equipment

Installation Items

Installation location(s): ____

____

Operational test frequency: ____

____

Operational test method: ____

____

System acceptance criteria: ____

____

Makes/models (CCTV display/recorders, alarm annunciation, card access control): ________________

____

Maintenance history/records: ____

____

CAS/SAS physical protection measures: ____

____

Tour/Visual Examination Items

Physical protection adequate? ____

____

Environmental controls/fire protection adequate? ____

____

Operator's console and controls layout accessible and functional? ________________________

____

All displays clear and readable? ____

____

SAS equipment sufficient? ____

____

Records storage adequate? ____

____

Sound level sufficient? ____

____

Data Collection Sheet
Alarm Processing and Display Equipment

Test Method

	Location Tested (CAS/SAS, Other)	Device/Equipment Tested	Function Tested	Type of Test (Functional Test, Historical Record Test, SAS Test)
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				

Comments:

Appendix B: Access Control System Performance Tests

Part 1

Personnel Access Control Equipment

Part 1

Personnel Access Control Equipment

Objective

The objective is to test the effectiveness of equipment (that is, card readers, remote closed circuit television [CCTV] identification hardware, and biometric systems) used to control access to security areas or used to supplement other access controls (for example, badge checks).

U.S. Department of Energy (DOE) orders require that only authorized personnel be allowed to access security areas. Also, the identity of personnel entering a Protected Area (PA), material access area (MAA), or Limited Area (LA) must be verified. The use of devices such as card readers and biometric or CCTV identification systems is not mandatory; such devices may be used to complement security police officer (SPO) badge checks or as a standalone system. (At PAs, SPOs must administer the access controls. This requirement has generally been interpreted to mean that the use of unattended access control systems at PAs is prohibited.)

System Tested

System:	Access control system
Functional Element:	Personnel authorization, identification, and verification
Component(s):	Card readers, CCTV identification systems, biometric identifiers (for example, hand geometry, retinal scans, voice recognition), transmission lines, access control central processing equipment, and interfaces with CCTV and central alarm station (CAS) operation; testing and maintenance of access control equipment

Scenario

Assessors should select one or more security area portals for testing. The selection is based on several factors, including portal configuration and location, operating history, number of portals, type of security areas where access control devices (ACDs) are used, and the type of devices used (for example, card reader, biometric system, CCTV). Assessors should look for potential deficiencies or misapplication of technology. Before testing the devices, the assessors should clearly understand how the access control systems function and what features are used at each portal. The assessors should observe the facility's security alarm technicians or SPOs as they conduct routine operational and sensitivity testing of selected devices. Assessors should select devices for testing based on the number, type, configuration, deployment, and operational history. When observing the testing of devices, assessors should note the procedures used to determine whether test and maintenance procedures are consistent with DOE orders and approved Site Safeguards and Security Plans (SSSPs), and whether the procedures are an effective means of testing the systems.

Assessors accomplish two goals by having the facility's security technicians conduct routine testing. First, these tests indicate the effectiveness of the facility test and maintenance program. Assessors can observe the test procedures to determine whether they are effective and, at the same time, determine whether the tested devices are operational. Second, facility testing should verify that devices are functional according to facility specifications, ensuring that the assessors will be testing a system that is operating as the facility intends. The effectiveness of the facility test program may be important in identifying the root cause of deficiencies.

If the facility does not test all features of the devices, the assessors may conduct their own testing, as appropriate. Tests are conducted to determine whether the devices function as intended and whether an adversary could exploit design or operational deficiencies and gain access to a security area without proper authorization.

The assessors should monitor the annunciation in the CAS, in the secondary alarm station (SAS), or at the portal, depending on the system design. The assessors can also observe the operation of interfacing systems, including automatic CCTV display, video recorders, and the CAS operators.

The number of portals and devices selected for testing depends on the time available, the importance of the system in the overall protection program, and the variation in individual portals. The following guidelines are intended to assist assessors in selecting sensors and zones for testing:

- Test at least two portals. If the portals use different types of devices, or if the device configuration at each portal is significantly different, assessors should consider selecting at least one of each type.

- Test at least one of each type of device if the devices are used for protecting high-priority targets such as Category I quantities of special nuclear material (SNM).

- If the first few tests do not indicate problems and there is no evidence of exploitable deficiencies, the assessors should not devote extensive time to testing numerous other portals or devices. However, if there are deficiencies, assessors should collect sufficient data to determine whether the deficiencies represent isolated problems or whether they are systemic.

- Assessors should conduct tests at portals in which deficiencies were noted on initial tours. For example, assessors may note that there are no apparent means of verifying that only one person at a time enters an unattended LA portal where card readers are used to control access; in such cases, the assessors should conduct tests to determine whether this situation could be exploited by an adversary.

Evaluation

For the access control system to be effective, the combination of hardware and procedural controls must be sufficient to prevent unauthorized entry to security areas. This section deals primarily with evaluating the ACDs, specifically card readers, biometric identifiers, and CCTV identification systems. Included are guidelines for assessing device performance and interpreting results in the context of system performance.

Assessing Equipment Performance

The primary objective in evaluating an ACD is to determine whether the device effectively and reliably discriminates between authorized and unauthorized access attempts, and whether it denies unauthorized access. The following questions should also be asked:

- Is the device a standalone system, or is it used in conjunction with a badge check or another means of access control?

- Are there provisions for visually monitoring (either directly or by CCTV) the portals where ACDs are used?

- Will an alarm be initiated if the portal door is forced open or opened from the inside in an unauthorized manner, and where does it report?

- Can the portal be bypassed (for example, by climbing over the portal into the security area) without creating an alarm/condition?

- Will power outages cause equipment failures that will impact security?

- Will an alarm condition be annunciated if a person is denied access authorization after a specified number of access attempts?

- Are there provisions to prevent "piggybacking" or unauthorized use of another person's credentials?

Interpreting Results

The following guidelines are provided to assist assessors in interpreting results:

- An access control system usually consists of multiple layers. Each layer is only as good as its weakest link. Tests that indicate that a knowledgeable adversary could enter the security area without authorization or detection through one or more portals are evidence that the access controls are ineffective. The significance of this deficiency must be analyzed in the context of the site-specific protection objectives and the effectiveness of complementary systems.

- Tests sometimes indicate that a device can be defeated but that, because of the degree of redundancy in the portal configuration, an adversary entering the security area would also have to defeat multiple security devices or other controls (for example, a badge check). In such cases, the identified deficiencies are less serious because of the defense-in-depth employed. However, the deficiencies may indicate design or testing and maintenance problems.

- Facility tests may indicate that the system is functional even though assessor testing indicates that the devices can be defeated. In such cases, the assessor can reasonably conclude that there are deficiencies in the test procedures or the quality assurance program.

- Facility tests indicating that devices are functional, in conjunction with assessor tests confirming that the devices are effective, are evidence that the tested portions of the system are effective and that test and maintenance procedures are also effective. However, the limitations of the tests must be recognized. For example, all modes of defeat (for example, piggybacking) may not have been fully tested.

Special Considerations

Related tests or activities, such as testing of search equipment or communications equipment, are typically conducted concurrently with the testing of devices.

Responsibilities

Assessors: Select the portals and devices. Direct tests and monitor alarm annunciation. (Typically one assessor will be stationed at the CAS and at least one at the portal.)

Facility: Conduct routine tests. Provide security technicians. Provide test devices as necessary (for example, coded cards for card-reader tests), and provide SPOs for security during tests as required. Provide radios for two-way communication.

Internal Coordination

Testing of devices should be scheduled to avoid conflicts with other tests involving the protective force.

Security Considerations

Observe all normal security considerations. Normally, an SPO must monitor (directly or by CCTV) tests to ensure that no unauthorized personnel enter the PA.

Personnel Assignments

Test Director:

Facility Alarm System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- Security technicians.

Equipment:

- Radios
- Test devices.

Safety:

- Follow normal operating procedures.
- Complete a safety plan.
- Notify the CAS and other alarm monitoring stations before testing is conducted.
- Station one assessor in the CAS.
- Coordinate with protective force personnel to prevent any undesired armed response to alarm signals.

CCTV Identification System

System Description:	CCTV systems are used to verify the identity of personnel entering a security area. Such systems allow a remotely stationed SPO to conduct a badge check by simultaneously viewing images of a person and his/her badge. Alternatively, the SPO may compare a person's image to a stored video image.
Components of CCTV Identification System:	Camera, transmission lines, monitor, remote door lock activator, electric door lock

Concerns

- CCTV identification systems do not include provisions for searching personnel and are not suitable for portals where searches are required.

- If SPOs do not pay adequate attention to verifying identity, unauthorized personnel may be allowed entry.

- Remote CCTV identification systems are vulnerable to persons disguising their faces or using false or stolen credentials. Therefore, these systems are not suitable for high-security purposes (for example, MAAs or PAs), but may be adequate for compartmentalizing areas within a security area.

- Uneven lighting, shutdown, glare, or degraded equipment may drastically reduce the capability to effectively compare images.

- If the CCTV identification system (or related controls) does not include provisions for preventing "tailgating" or piggy-backing (two or more persons entering an area using only one credential), the facility may be vulnerable to insiders deliberately allowing access, or employees unwittingly allowing access, to unauthorized persons. Measures to deter tailgating include having SPOs monitor the area or using mantraps (interlocked doors or turnstiles designed to ensure that only one person passes through at a time).

- Cameras and related systems and monitors require periodic maintenance to ensure reliable operation.

- Systems without uninterruptible or auxiliary power will not operate in the event of a power failure. Facilities with systems that fail in the non-secure mode (for example, electric locks that fail in the open position) may be vulnerable to unauthorized access during periods when power is unavailable because of natural events, accidents, or deliberate sabotage.

Types of Tests

- Electric Door Lock Tests

  One test involves verifying that the door lock engages immediately after the door closes so that a person following immediately behind cannot open the door before the door lock engages. The assessors should examine the door and electric lock system to determine whether it can be defeated by techniques such as blocking the lock operation or cutting power to magnetic locks.

- Door Alarm Interface Tests

  These tests are conducted to determine whether the door alarm is operational and integrated with the remote control. One such test is to hold the door open for an extended period (that is, 30 seconds or more) to determine whether an alarm condition is initiated. This test is usually applicable only at unattended doors.

- Visual Examination of CCTV Monitor

  The assessors should enter the CAS, SAS, or other location where a CCTV identification monitor is located and observe image quality. If any CCTV identification portals are outdoors, observation of monitors under day and night conditions is recommended.

Test Guidelines

- The most frequent problem with CCTVs is improperly maintained equipment. The assessors should visually check the quality of the images on the monitors at the CAS, SAS, and other control locations.

- Tests of electric door locks or door alarm interfaces should be conducted at portals that are used for high-security application and are not protected by other means (for example, SPOs stationed at the post who can monitor the entrance).

- Tests involving unauthorized personnel or persons using improper credentials may be designed to test the alertness of the SPOs who monitor the CCTV identification system. However, such tests must be conducted without the knowledge of the SPO and require detailed safety plans.

Checklist

CCTV Identification System

Access Control Equipment

Interview Items

Installation location: ____

____

Maintenance frequency and procedure: ____

____

Type of lock controlled by card reader (if any): ____

____

Enrollment procedures (video comparator only): ____

____

De-enrollment procedure (video comparator only): ____

____

Alternative means of granting access: ____

____

Tour/Visual Examination Items

Environmental protection: ____

____

SPO capability to monitor door and passageway: ____

____

Mantrap or turnstile configuration: ____

____

Door lock configuration: ____

____

Door alarm configuration: ____

____

Quality of image in monitor: ____

____

Data Collection Sheet
CCTV Identification System

Test Method

	Zone Tested	Zone Number	ID System	ID Confirmation Method	Electric Door Locks	Door Alarm Interface	Special Features
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							

Comments:

Card-Reader Systems

System Description:	Card readers and coded credentials are used to supplement or replace badge checks as a means of access control. The coded credential may be a separate card or it may be imbedded in a photograph identification badge. The coded credential may be used alone or in conjunction with a biometric device or a Personnel Identification Number (PIN). The card reader may be used to operate electric locks and/or provide information to an SPO at the post.
Coded Credential Technologies:	Optical Bar code Magnetic – spot Magnetic – stripe Wiegand effect Proximity Capacitance Smart cards
Components of Card Reader:	Card reader, electric lock, coded credential, central controller, printer, enrollment console, PIN keypads, transmission lines, multiplexors, tamper indicators (switches or line supervision)
Features of Card Reader Systems (not all systems have all features):	Time zone Area zone Anti-passback Occupant listing Fail soft Operator manual override

Concerns

- A card-reader system alone does not verify the identity of a person. Card-reader systems are not acceptable as standalone systems for high-security applications including PAs, MAAs, and LAs. Additional controls, such as badge checks, remote CCTV identification, or biometric identification, are necessary to verify that the person who possesses a coded credential is authorized to enter an area. Standalone card-reader systems may be an acceptable means of controlling access to rooms or areas within a larger security area in an effort to enhance security by compartmentalization.

- Most coded credentials can be decoded or counterfeited by using the appropriate equipment and information. If credentials are lost, stolen, compromised, or not voided (that is, deleted from the system) in a timely manner, the potential for adversaries to use such credentials increases. Also, adversaries may obtain a credential from an authorized person by force, stealth, deceit, or through the voluntary or coerced assistance of an insider.

- If the card-reader system (or related controls) does not include provisions for preventing tailgating (two or more persons entering an area using only one credential), the facility may be vulnerable to insiders deliberately allowing access, or employees unwittingly allowing access, to unauthorized persons. Measures to deter tailgating include having SPOs monitor the area or using mantraps (arrangements of interlocked doors or turnstiles designed to ensure that only one person passes through at a time).

- If the card-reader system (or related controls) does not include provisions for preventing pass-back (for example, an authorized person enters an area and passes his/her card back to another person, who then enters the area), the facility may be vulnerable to insider actions. Measures to deter pass-back include mantraps, effective lane control, monitoring by SPOs, and anti-pass-back features associated with the card-reader system.

- Card readers require periodic maintenance to ensure reliable operation. Card readers located outdoors require more frequent maintenance.

- Card readers that do not have a means of detecting tampering (for example, tamper switches and line supervision or continuous SPO monitoring) may be susceptible to defeat.

- If the authorized access lists are not reviewed and updated frequently (by deleting the credentials), persons who no longer have a need to access the area could enter that area. Similarly, if there is a lag time between the time when a person is no longer permitted access (for example, the individual is reassigned or terminated) and the time his/her access credentials are actually deleted (de-enrollment), a window of vulnerability exists.

- Systems without uninterruptible or auxiliary power will not be operational in the event of a power failure. Facilities with systems that fail in the non-secure mode (for example, electric locks that fail in the open position) may be vulnerable to unauthorized access during power outages (due to natural events, accidents, or deliberate sabotage).

- Facilities that have enrollment procedures that do not include provisions for verifying the enrollment request may be vulnerable to unauthorized enrollment.

- Facilities with enrollment procedures that do not ensure that only authorized personnel enroll or delete credentials, or do not include provisions for supervisory approval (or other procedures to verify that only proper credentials are enrolled), may be vulnerable to the employees (particularly those who operate the enrollment system) acting as insiders.

- PINs may be compromised if PIN keypads are not designed to prevent bystanders from observing the PIN entry.

- Fail-soft features (operation in a degraded mode with a lower level of security) may degrade access controls if other hardware or procedural controls are not used in conjunction with the badge reader.

Types of Tests

- Improper Card Tests

  These tests are conducted to verify that access is not allowed (for example, door is not opened) when an invalid card is used. Repeated failures to access should result in an alarm for those systems equipped to detect repeated, unsuccessful access attempts.

- Tamper Alarm Tests

  In these tests, card readers, multiplexors, or junction boxes are opened to test tamper switches. Alarm wires are shorted to test line supervision. Testing should be conducted in both access and secure modes if the entrance is so configured.

- Electric Door Lock Tests

  One test involves verifying that the door lock engages immediately after the door closes so that a person following immediately behind cannot open the door before the door lock engages. Assessors may also examine the door and electric lock system to determine whether it can be defeated by techniques such as blocking the lock operation or cutting power to magnetic locks. This test is only applicable at unattended doors that are controlled by card-reader systems.

- Door Alarm Interface Tests

  These tests are conducted to determine whether the door alarm is operational and integrated with the card-reader control. One such test is to simply hold the door open for an extended period (for example, 30 seconds or more) and determine whether an alarm condition is annunciated. This test is usually only applicable at unattended doors.

- Special Features Tests

  Special features, such as time zoning or anti-passback capability, must be tested. Assessors should attempt to use a card in a manner that should not result in access being granted. For example, the assessor can enter an MAA, exit that MAA without reading out, attempt to enter the MAA again (or attempt to enter a second MAA), and verify that access is denied or an alarm condition initiated.

Test Guidelines

- Card-reader systems tend to operate reliably and rarely fail in a non-secure mode if designed properly. The tests are conducted primarily to verify information about system capabilities or features, so a small number of tests are usually sufficient. Testing that involves an improper card and testing of tamper alarms should be performed at two or three portals.
- Special features, if required, may be tested as appropriate for the site-specific system. Such testing requires the assessor to understand the system's features and how they are implemented (for example, the card readers at an MAA entrance may use different features than those at a PA entrance or a different MAA).
- Interface with the door lock or alarm is the most common problem with card-reader systems. Testing of door locks or door alarm interfaces should be conducted at portals that are used for high-security application and are not protected by other means (for example, SPOs stationed at the post who can monitor the entrance).

Checklist

Card-Reader Systems

Access Control Equipment

Interview Items

Installation location: ____

____

Operational test frequency and method: ____

____

Maintenance frequency and procedure: ____

____

False alarm history/records: ____

____

Tamper alarm (switches or line supervision): ____

____

Mode of operation (standalone or as a supplement to SPOs) at different locations: ______________

____

Technology of coded credential (for example, bar code): ___________________________________

____

Use with PIN or biometric device: ____

____

Type of lock controlled by card reader (if any): ____

____

Enrollment procedures: ____

____

De-enrollment procedure (lag time): ____

____

Card-Reader Systems

Time zoning: ____

____

Area zoning: ____

____

Anti-passback: ____

____

Occupant listing: ____

____

Fail-soft: ____

____

Operator manual override: ____

____

Visual Examination Items

Environmental protection: ____

____

SPO capability to monitor door and passageway: ____

____

Mantrap or turnstile configuration: ____

____

Door lock configuration: ____

____

Door alarm configuration: ____

____

Data Collection Sheet
Card-Reader Systems

Test Method

	Zone Tested	Zone Number	Card Type	Improper Card	Tamper	Electric Door Lock	Door Alarm Interface	Special Features
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								

Comments:

Biometric Identifiers

System Description:	Biometric devices are used to verify identity based on some unique physical characteristic of the individual. Biometric devices may be used as a standalone system or in conjunction with other controls such as card readers, PINs, or badge checks. The biometric device may be used to operate electric locks and provide information to an SPO.
Biometric Technologies:	Voice verification Eye-retinal pattern verifier Fingerprint verifier Hand geometry
Components of Biometric ID Systems (not all systems have all features):	Biometric device, electric lock, central controller, printer, enrollment console/device, PIN keypads, transmission lines, multiplexors, tamper (switches and line supervision)
Features of Biometric Device Systems (not all systems have all features):	Time zone Area zone Fail-soft Occupant listing Operator manual override

Concerns

- Biometric devices are used at only a few DOE facilities. Retinal scan and hand geometry devices are the most commonly used. If properly applied, the use of biometric devices can be a significant strength.
- Some facilities have problems with their devices frequently rejecting authorized users. Alternative verification procedures that provide an acceptable level of security should be available to avoid unacceptable impacts on operations.
- Some types of devices can be fooled, if repeated attempts are allowed. The system should be designed to detect successive rejections that may indicate an imposter is attempting to match a biometric template. Provisions should also be made to monitor the portal directly or by CCTV to minimize the potential for tampering with the system or using a fabricated or forged biometric sample.
- If the biometric device system (or related controls) does not include provisions for preventing tailgating (two or more persons entering an area using only one credential), the facility may be vulnerable to insiders deliberately allowing access, or employees unwittingly allowing access, to unauthorized persons. Measures to deter tailgating include having SPOs monitor the area or using mantraps (arrangements of interlocked doors or turnstiles designed to ensure that only one person passes through at a time).
- Biometric devices require periodic maintenance to ensure reliable operation.
- Biometric devices that do not have a means of detecting tampering (for example, tamper switches and line supervision or continuous SPO monitoring) may be susceptible to defeat.
- If the authorized access lists are not reviewed and updated frequently (by deleting the person's authorization), persons who no longer have a need to access the area could enter that area. Similarly, if there is a lag time

between the time when a person is no longer permitted access and the time his/her access credentials are actually deleted (de-enrollment), a window of vulnerability exists.

- Systems without uninterruptible or auxiliary power will not be operational in the event of a power failure. Facilities with systems that fail in the non-secure mode (for example, electric locks that fail in the open position) may be vulnerable to unauthorized access during power outages (due to natural events, accidents, or deliberate sabotage).

- Facilities with enrollment procedures that do not include provisions for verifying the enrollment request may be vulnerable to unauthorized enrollment.

- Facilities with enrollment procedures that do not ensure that only authorized personnel enroll or delete credentials, or do not include provisions for supervisory approval (or other procedures to verify that only proper credentials are enrolled), may be vulnerable to employees (particularly, those who operate the enrollment system) acting as insiders.

- PINs may be compromised if PIN keypads are not designed to prevent bystanders from observing the PIN entry.

- Fail-soft features (operation in a degraded mode with a lower level of security) may degrade access controls if other hardware or procedural controls are not used in conjunction with the badge reader.

Types of Tests

- Attempted Entry by Unauthorized Person

  This test is conducted to verify that an unauthorized person who attempts to enter is not allowed access. Repeated access attempt failures should result in an alarm for those systems equipped to detect repeated, unsuccessful access attempts.

- Tamper Alarm Tests

  In these tests, biometric devices, multiplexors, or junction boxes are opened to test tamper switches. Alarm wires are shorted and opened to test line supervision. Testing should be conducted in both access and secure modes if the portal is so configured.

- Electric Door Lock Tests

  One test involves verifying the door lock engages immediately after the door closes so that a person following immediately behind cannot open the door before the door lock engages. The assessors may also examine the door and electric lock system to determine whether it can be defeated by techniques such as blocking the lock operation or cutting power to magnetic locks. This test is only applicable at unattended doors that are controlled by card-reader systems.

- Door Alarm Interface Tests

  These tests are conducted to determine whether the door alarm is operational and integrated with the card-reader control. One such test is to simply hold the door open for an extended period (that is, 30 seconds or more) and determine whether an alarm condition is initiated. This test is usually only applicable at unattended doors.

- Special Features Tests

  Special features, such as time zoning or anti-passback capability, must be tested. Assessors should attempt entry in a manner that should not result in access being granted. For example, assessors should enter an MAA, exit that MAA without reading out, attempt to enter the MAA again (or attempt to enter a second MAA), and verify that access is denied or an alarm condition initiated.

Test Guidelines

- Biometric device systems tend to operate reliably and rarely fail in a non-secure mode if designed properly. The tests are conducted primarily to verify information about system capabilities or features. Thus, a small number of tests are usually sufficient. Tests involving attempted entry by an unauthorized person and tests of tamper alarms should be performed at two or three portals.

- Special features, if required, may be tested as appropriate for the site-specific system. Such testing requires the assessor to understand the system's features and how they are implemented (for example, the biometric devices at one MAA entrance may use different features than those at a second MAA).

- Interface with the door lock or alarm is the most common problem with biometric systems. Testing of electric door locks or door alarm interfaces should be conducted at portals that are used for high-security applications and are not protected by other means (for example, SPOs stationed at the post who can monitor the entrance).

Checklist

Biometric Identifiers

Access Control Equipment

Interview Items

Installation location: ____

____

Operational test frequency and method: ____

____

Maintenance frequency and procedure: ____

____

False alarm history/records: ____

____

Tamper alarm (switches or line supervision): ____

____

Mode of operation (standalone or as a supplement to SPOs) at different locations: ______________________

____

Technology (for example, retinal scan): ____

____

Used with PIN or card reader: ____

____

Type of lock controlled by biometric device system: ____

____

Enrollment procedures: ____

____

De-enrollment procedure (log time): ____

____

Biometric Device System Features

Time zoning: ____

____

Area zoning: ____

____

Occupant listing: ____

____

Fail-soft: ____

____

Operator manual override: ____

____

Visual Examination Items

Environmental protection: ____

____

SPO capability to monitor door and passageway: ____

____

Mantrap or turnstile configuration: ____

____

Door lock configuration: ____

____

Door alarm configuration: ____

____

Data Collection Sheet
Biometric Identifiers

Test Method

	Zone Tested	Zone Number	Biometric Identifier	Unauthorized Entry	Tamper Alarm	Electric Door Lock	Door Alarm Interface	Special Features
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								

Comments:

Part 2

SNM Detectors

Part 2

SNM Detectors

Objective

The objective of these limited-scope performance tests is to determine the effectiveness of SNM detectors to detect the unauthorized removal of SNM through an access control portal.

System Tested

System:	Access control system
Functional Element:	Exit search
Component(s):	Detectors (hand-held, portal, vehicle), including signal processing equipment and annunciation equipment; testing and maintenance of detectors

Scenario

The assessors should select one or more SNM detectors for testing. This selection is based on several factors, including portal configuration and location, operating history, the number of portals, the different types of SNM detectors in use (vehicle, walkthrough, hand-held), and the types of locations where SNM detectors are used (PAs, MAAs, others).

The assessors should then observe the facility's security alarm technicians or SPOs as they conduct the routine operational or sensitivity tests of selected SNM detectors. During this portion of the test, the assessors should observe the test procedures used in order to determine whether the tests, calibrations, and maintenance procedures are consistent with DOE orders and approved SSSPs, and whether they are an effective means of testing the systems.

Two goals are accomplished by having the facility's security technicians conduct routine testing prior to testing by assessors. First, the facility tests indicate the effectiveness of the test and maintenance program. Assessors can observe the test procedures to determine whether they are effective and have an opportunity to determine whether the selected SNM detectors are properly calibrated. Second, the facility's tests should verify that the detectors are calibrated according to facility specifications to ensure that the assessors will be testing a system that is operating as the facility intends. This may be important in identifying the root cause of deficiencies.

The assessors should then conduct operational and sensitivity testing as appropriate for the type of detectors in use. The purpose of these tests is to determine whether the detectors are properly calibrated and whether they are sensitive enough to meet site-specific protection objectives.

The number of detectors selected for testing depends upon the time available, the importance of the system in the overall protection program, and the variety of detectors used at different portals. The following guidelines are intended to assist the assessor in selecting detectors for testing:

- At very small facilities, or at facilities with fewer than five SNM portals, the assessors may choose to test detectors at each portal. At larger facilities, the assessors would typically select two to four portals for testing.

- Because of the configuration of the security layers, at many facilities the exit searches at the MAAs are more critical for protecting SNM than those at PAs or outer security areas. Consequently, focusing efforts on the SNM detectors at MAA portals is often appropriate. However, SNM detectors at PA portals should not normally be completely neglected.

- Normally, the assessors should test at least one of each type of detector (that is, hand-held, vehicle, walkthrough). However, the assessors need not test each type of detector at each portal selected.

- If the first few tests do not indicate problems and there is no evidence of exploitable deficiencies, the assessors should not generally devote extensive time to testing numerous additional detectors. However, if deficiencies are apparent, the assessors should collect sufficient data (by testing additional detectors) to determine whether a deficiency is an isolated instance or evidence of a systemic problem. Also, if testing indicates that detectors are not sufficiently sensitive to detect the goal quantity of SNM, the assessors may elect to repeat testing with larger sources (if available) to determine the magnitude of the deficiency.

Evaluation

If exit searches are to be effective, the SNM detection equipment must be part of an integrated system consisting of hardware, personnel, and procedures. This section deals primarily with the evaluation of the SNM detector hardware. Guidance is provided on assessing detection effectiveness and on interpreting results in the context of system performance.

The primary objective in evaluating an SNM detector is to determine whether the unit effectively and reliably detects the passage of a determined quantity of SNM through the detection zone. The following points should also be considered in the evaluation:

- Are there provisions for monitoring personnel, packages, or vehicles passing through the detection zone to ensure that normal procedures are followed? For example, are there provisions for ensuring that personnel:

  – Do not bypass the detector zone?
  – Do not throw items through the detection zone?
  – Do not pass through walkthrough monitors at an unusually high rate of speed (that is, running instead of walking)?
  – Do not pass items through walkthrough monitors at an extremely slow speed?
  – Do not drive through vehicle detector zones at an unusually high speed?
  – Follow all site-specific procedures?

- Is the system of barriers and procedures at the SNM portal sufficient to ensure that material is not passed around the detector?

- Are there adequate provisions for detecting shielded SNM (that is, metal detectors used in conjunction with SNM detectors)?

- Are the SPOs who monitor the SNM detectors trained in using the equipment, and are they familiar with the search procedures?

- Are SNM detector alarm response procedures clear, complete, and sufficient to ensure that all anomalies are resolved prior to allowing egress?

- Are provisions adequate to ensure that unauthorized personnel do not tamper with the SNM detection equipment and do not have access to control settings?

- Do the detectors have features, such as high- and low-background alarms, that alert the protective force to conditions that could alter detection capability? If not, are alternate measures in place to provide adequate assurance?

- Are testing and maintenance procedures sufficient to ensure that the detectors are reliable and correctly calibrated?

- Have the test sources been selected with appropriate consideration of the type and form of SNM in the security area?

- Do the test procedures include all aspects of detector operation, including tests of high-background alarms, low-background alarms, and occupancy sensor operation?

- If plutonium sources are used for testing, are there provisions to ensure that only low burn-up plutonium test sources are used?

Interpreting Results

The following guidelines are provided to assist the assessors in interpreting results in the context of system performance.

- Testing that indicates that the SNM detectors can be bypassed or do not reliably detect removal of significant quantities of SNM (that is, significantly greater than the goal quantity) is evidence of a potentially serious deficiency. The significance of such deficiencies must be analyzed in the context of site-specific protection objectives and the effectiveness of other complementary systems. In general, deficiencies in SNM detectors at a portal are most significant at facilities that have Category I or II quantities of SNM in portable forms and that rely on a single layer of exit search. Potential factors that may partially mitigate deficiencies in SNM detection equipment are additional layers of exit searches; material controls that provide high assurance that material is not diverted; and SNM in forms (for example, large pieces or irradiated) that are less likely to be successfully diverted.

- Testing that indicates a slight miscalibration or detector drift is significant, but much less serious than gross miscalibrations or exploitable deficiencies. For example, testing may indicate the goal quantity (for example, 10 grams U-235) could be passed through the detector at shoe level eight out of ten tries at one facility portal. Additional testing may indicate a slightly larger test source (for example, 15 grams U-235) could be reliably detected (for example, ten out of ten passes). Such results would indicate a miscalibrated sensor, but not a serious vulnerability. However, these results also indicate a possible testing and maintenance deficiency. The assessors should consider conducting additional tests in order to determine whether the miscalibration is an isolated case or a systemic problem.

Special Considerations

DOE Office of Enterprise Assessments assessors do not possess radioactive test sources and must use test sources provided by the facility. The assessors should contact the facility point of contact early in the planning process to determine what types and sizes of test sources are available.

SNM detectors should be tested by using the type of SNM that is located within the security area (for example, plutonium sources in plutonium processing areas and uranium sources in uranium processing areas).

Occasionally, the facility will conduct testing and calibration activities using a different type of source (for example, barium or cesium) and will not have a uranium or plutonium source. In such cases, assessors should determine whether a standard uranium or plutonium source can be obtained or whether small quantities of the SNM used in the facility's process lines can be used to test the detectors.

Related testing and activities, such as metal detector tests and reviews of portal barriers and procedures, are typically conducted concurrently with SNM detector testing to increase the efficiency of data gathering.

Responsibilities

Assessors: Select the portals and detectors. Direct testing and monitor alarm annunciation.

Facility: Conduct routine tests. Provide test sources. Assign SPOs to provide security during testing, as required. Provide security technicians to conduct testing at the direction of the assessors.

Internal Coordination

Testing should be scheduled to avoid conflicts with other tests involving the protective force. Testing should be coordinated with the material control and accountability (MC&A) topic team (if any) to avoid duplication of effort.

Security Considerations

Observe all normal security considerations. Normally, a protective force representative must monitor testing to ensure that security is maintained.

Personnel Assignments

Test Director:

Facility Alarm System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- Alarm technicians.

Equipment:

- Test sources
- Shielding material (as needed).

Safety:

- Follow normal operating procedures.
- Complete a safety plan.
- Notify the CAS and other alarm monitoring stations before testing.
- Station one assessor in the CAS.
- Coordinate with protective force personnel to prevent any undesired armed response.

Definitions

Calibration procedure: Facility technicians use calibration test sources to calibrate detectors and to perform acceptance testing. For walkthrough monitors, these sources are sometimes ten grams U-235 or one gram plutonium. The calibration procedures typically call for the calibration source to be passed through the detector at normal walking speed at selected locations. The acceptance criterion is 50 percent detection probability with 95 percent confidence, although some facilities use a more stringent criterion for calibration purposes.

Detection zone is the area where the detectors are designed to effectively detect SNM. For walkthrough or vehicle detectors, the detection zone is the area between the detectors. For hand-held detectors, this is the area exposed to the detector during the search procedures.

Goal quantity is the amount of SNM that is to be reliably detected when passed through the detection zone and may be defined on a site-specific basis with DOE field element approval. Traditionally, standard test sources are ten grams U-235 or one gram plutonium, which should be detected anywhere in the detection zone with 50 percent detection probability at 95 percent confidence when the source is passed through the detector at normal walking speed. The assessors should assume these test sources are the goal quantity unless the facility has identified, justified, and documented an alternative site-specific goal quantity in an approved SSSP. A goal quantity defined by a facility would typically be larger than the calibration source. The larger goal quantity may be justified on the basis of the type of SNM in the security area (that is, no bulk material or small pieces) or in consideration of the other material controls and detection mechanisms that would likely prevent an adversary from removing a large quantity of SNM (that is, Category I or II) from a security area by diverting small amounts of SNM (less than a goal quantity) over an extended period. For example, if the goal quantity is 20 grams of U-235, it would take 250 diversions of 20 grams to accumulate a Category I quantity of uranium metal.

SNM Detector—Walkthrough Testing

Typical Uses

- To detect SNM at MAA personnel egress points
- To detect SNM at PA personnel egress points.

Concerns

- Personnel are typically in the detection zone of a portal monitor for only a short time, and detection capability is sensitive to the rate of speed at which they pass through the detectors. The detectors are typically calibrated and tested with a test source carried by a person who walks through the detector at a normal rate of speed. If the speed of exiting personnel is not adequately controlled (that is, if personnel are not prevented from running or throwing items through the detectors), the detection capability can be substantially reduced.

- Detectors, wiring, and electronics may be susceptible to tampering if they are not adequately protected by methods such as buried lines, locked control panels, or tamper alarms.

Types of Tests

- Operability Tests

  These tests are conducted to verify proper operability of the detector and simply involve walking through the detection zone with a goal quantity of SNM or the standard test source according to the normal procedures at that post (which may include requirements for a short pause before proceeding). Such testing should be conducted with the source placed near the left edge, center, and right edge of the detection zone and at different elevations (for example, shoe level, waist level, head level).

- Sensitivity Tests

  Sensitivity tests are conducted to determine whether the detector is correctly calibrated. Such testing generally involves observing a security technician as he/she conducts the acceptance test that would normally be conducted after a calibration.

  Sensitivity tests may involve a series of walkthroughs designed to demonstrate that the detector has an acceptable detection probability.

- High-Background Tests

  High-background tests are conducted to verify that high-background alarms operate as designed. Generally, the facility's or manufacturer's test procedures are followed. Testing typically involves slowly moving a radiation source toward the SNM detector (without setting off the occupancy sensor) while monitoring the detector count rate in order to verify the high-background alarm occurs at the specified threshold value.

- Low-Background Tests

  Low-background tests are conducted to verify that low-background alarms operate as designed. Generally, the facility's or manufacturer's test procedures are followed. Testing typically involves disabling or shielding the detectors to reduce the count rate. The assessors monitor the count rate to verify that the alarm occurs at the specified threshold.

- Occupancy Sensor Tests

  SNM detectors use a variety of occupancy sensors to detect the presence of personnel and to initiate the monitoring measurement. The most commonly used sensors include photoelectric, ultrasonic, microwave, infrared, and pressure sensitive. Occupancy sensors are tested to verify sensor operability. Generally, the facility's or manufacturer's test procedures are followed and typically involve entering the detection zone and verifying the alarm.

- SNM Detection Capability Tests

  Assessors may elect to conduct additional testing of detection sensitivity, focusing on the capability of the detectors to detect SNM removal. Such testing may involve using SNM in the form and quantity found in the security area and testing the detection capability with the SNM concealed at various locations on the body, or in packages. The assessors should use their knowledge of SNM detectors, occupancy detectors, and search procedures to conduct tests that will challenge the system. For example, assessors can attempt to pass material through the walkthrough monitor while avoiding the occupancy sensor. Another example is a "kick test," which involves placing the SNM at shoe level and swinging the foot through the detector as fast as possible when walking through (minimizing the time in the detection zone). Testing should be conducted with a quantity of SNM that is equal to or greater than the goal quantity.

- Shielded SNM Tests

  Assessors may elect to conduct testing of the detector's capability to detect shielded SNM. Such tests involve shielding SNM with lead or other shielding material. Assessors can then determine the amount of shielding that is necessary to prevent detection of a significant quantity of SNM (for example, a Category I quantity). Any quantity of SNM can be shielded and detection prevented if a sufficient amount of shielding is used. Shielding tests can be used to determine how much shielding would be necessary. Such information can be used to determine whether the other search procedures (for example, visual observation as the person passes through the portal) are a credible means of detection, and can also be used as a baseline for performance tests of SPO search procedures. For example, if shielding tests indicate that a 20-pound lead container will prevent detection of a Category I quantity of SNM, then the assessors might conduct testing of the SPO's visual search procedures involving a lead container in a toolbox.

Test Guidelines

- Typically, the assessors conduct operability tests, sensitivity tests, high-background tests, low-background tests, and occupancy sensor tests at a few key portals (usually two or three). If the facility has a large number of portals and those portals use several different types of detectors or substantially different search procedures, then the assessors may choose to test one of each major type of portal detector.

- SNM detection capability tests and shielded SNM tests should be conducted at a typical portal if an appropriate SNM source and shielding is available. Frequently, such tests require extensive security precautions, particularly if Category II or greater quantities of SNM are involved. The assessors may, instead, elect to review the results of similar tests or analyses conducted by the facility to determine the capability to detect SNM in shielded or unshielded configurations.

- If any deficiencies are noted in the installation or operation of detectors, or in the implementation of search procedures, the assessors should conduct testing to exploit those deficiencies in order to determine their significance/extent. For example, if the assessors note that a SNM walkthrough detector is not adequately monitored by SPOs, then the assessors could design and conduct tests to determine whether a person could

successfully throw a significant quantity of SNM through the detector in an attempt to avoid detection. Additional tests could be conducted to determine how large a quantity could be diverted by that method. Tests that are designed to indicate whether the SPO notes any unusual behavior (for example, throwing items through the detector) might be considered.

- If an individual detector can be defeated, that same detector should be tested again to determine whether such defeat is repeatable. Several tests of the same detector may be required to determine whether an adversary can exploit a deficiency.

- If an individual SNM detector can be defeated by one or more methods (for example, walk through, pass around), the similar SNM detectors at other portals should be tested by the same method in order to determine the extent of the problem. If possible, assessors should conduct several (three to five) more tests at different portals. If most of these tests indicate the detector can be reliably defeated, there is sufficient evidence that a systemic problem exists. If no other detectors are defeated, then one may conclude that an isolated deficiency was identified. If the results are inconclusive, the assessor should consider testing more detectors. Rarely would an assessor test more than five detectors by the same method.

- If the adversary has sufficient knowledge, time, and equipment, all SNM detectors can be defeated by using sufficient quantities of shielding. Testing should generally be conducted only if a portal is particularly vulnerable (for example, due to lack of metal detection capability) or if direct visual observation CCTV or SPOs at posts are considered inadequate to reasonably ensure that such attempts can be detected.

Checklist

SNM Detector

Walkthrough

Interview Items

Installation location: ____

____

Operational test frequency: ____

____

Operational test method: ____

____

Sensitivity test frequency: ____

____

Sensitivity test method: ____

____

False alarm history/records: ____

____

Make/model: ____

____

Tamper protection: ____

____

Provisions for personnel with medical conditions that cause alarms: ______________________________

____

Tour/Visual Examination Items

Control settings protected? ____

____

Occupancy sensor? ____

____

SPO monitoring method (CCTV, direct)? ____

____

One-way or two-way traffic? ____

____

Metal detector used? ____

____

Package search method? ____

____

Data Collection Sheet
SNM Detector—Walkthrough Monitors

Test Method

	Zone Tested	Portal Location	Operability	Sensitivity	Kick	High Background	Low Background	Occupancy Sensor	Detection	Shielded SNM	Other
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											

Comments:

SNM Detector—Vehicle Monitor

Typical Uses

- To detect SNM at MAA vehicular egress points
- To detect SNM at PA vehicular egress points
- To detect SNM at key roadways or badge check stations.

Types

- Portal Monitors—drive through during monitoring
- Monitoring Station—vehicle stationary during monitoring
- Hand-held—various types.

Concerns

- Vehicles are typically in the detection zone of a portal monitor for only a short time, and detection capability is sensitive to the rate of speed at which they pass through the detectors. The detectors are typically calibrated and tested with a test source in a vehicle that is moving through the detector at a normal rate of speed. If the speed of exiting vehicles is not adequately controlled (that is, if the vehicles are allowed to pass through the monitors at a rate significantly faster than that used for calibration), the detection capability can be reduced.

- Highly effective vehicle searches are difficult to achieve. Vehicle monitors are typically less sensitive than personnel monitors because of the greater distances between detectors. Further, vehicles are constructed from radiation-attenuating material and are capable of transporting large masses of shielding material. Facilities must attempt to strictly limit vehicular access to areas that have significant quantities of SNM. Also, failure to conduct a visual examination, concurrent with the vehicle monitor search, reduces the assurance that attempts to divert shielded SNM will be detected.

- Portal monitors are typically installed in housings six to eight feet tall. Large trucks can be considerably taller than the portal monitors. The capability to detect SNM concealed near the top of all vehicles may be reduced if no supplemental measures (such as visual searches or searches with hand-held detectors) are enacted for tall vehicles.

- Detectors, wiring, and electronics may be susceptible to tampering if they are not adequately protected by methods such as buried lines, locked control panels, or tamper alarms.

Types of Tests

- Operability Tests

  These tests are conducted to verify proper operability of the detector. They simply involve driving (or walking, assuming the vehicle occupancy detector can be activated) through the detection zone with a goal quantity of SNM or the standard test source. These tests should be conducted with the source placed near the left edge, center, and right edge of the detection zone.

- Sensitivity Tests

  Sensitivity tests are conducted to determine whether the detector is correctly calibrated. Such tests generally involve observing a security technician as he/she conducts the acceptance test that would normally be conducted after a calibration. This may involve a series of pass-throughs designed to demonstrate that the detector has an acceptable detection probability.

- High-Background Tests

  High-background tests are conducted to verify that high-background alarms operate as designed. Generally, the facility's or manufacturer's test procedures are followed. Testing typically involves slowly moving a radiation source toward the SNM detector (without setting off the occupancy sensor) while monitoring the detector count rate in order to verify that the high-background alarm occurs at the specified threshold value.

- Low-Background Tests

  Low-background tests are conducted to verify that low-background alarms operate as designed. Generally, the facility's or manufacturer's test procedures are followed. Testing typically involves disabling or shielding the detectors to reduce the count rate. The assessors monitor the count rate to verify that the alarm occurs at the specified threshold.

- Occupancy Sensor Tests

  SNM detectors use a variety of occupancy sensors to detect the presence of vehicles and to initiate the monitoring measurement. The sensors commonly used include photoelectric, microwave, infrared, pressure-sensitive, and metal detectors. Occupancy sensors are tested to verify sensor operability. Generally, the facility's or manufacturer's test procedures are followed. These typically involve entering the detection zone and verifying the alarm.

- SNM Detection Tests

  Assessors may elect to conduct additional tests of detection sensitivity, focusing on the capability of the detectors to detect SNM removal. Such tests may involve using SNM in the form and quantity found in the security area and testing the detection capability with the SNM concealed at various locations on the vehicle (for example, in the trunk, on the roof, or under the hood). The assessors should use their knowledge of SNM detectors, occupancy detectors, and search procedures to conduct testing that will challenge the system. For example, assessors can attempt to minimize the time the SNM is in the detection zone by placing the source near the front of the vehicle and driving through the detectors as fast as practical (while maintaining safety). Testing should be conducted with a quantity of SNM equal to or greater than the goal quantity.

- Shielded SNM Tests

  Assessors may elect to conduct tests of the detector's capability to detect shielded SNM. Such tests involve shielding SNM (in the form and quantity in the security area) with lead or other shielding material. Assessors can then determine the amount of shielding that is necessary to prevent detection of a significant quantity of SNM (for example, a Category I quantity). It is recognized that any quantity of SNM can be shielded and detection prevented if a sufficient amount of shielding is used. Shielding tests can be used to determine how much shielding would be necessary. Such information can be used to determine whether the other search procedures (for example, visual searches) are a credible means of detecting removal attempts, and can also be used as a baseline for performance tests of SPO search procedures. For example, if shielding tests indicate that a 100-pound lead container will prevent detection of a Category I quantity of SNM, then the assessors might consider conducting tests of the SPO's visual search procedures involving a "suspicious" 100-pound lead container in a vehicle.

Test Guidelines

- Typically, the assessors conduct operability tests, sensitivity tests, high-background tests, low-background tests, and occupancy sensor tests at a few key portals (typically two or three). If the facility has a large number of vehicle portals and those portals use several different types of detectors or substantially different search procedures, then the assessors may choose to test one of each major type of vehicle portal detector.

- SNM detection capability tests or shielded SNM tests should be conducted at a typical portal if an appropriate SNM source or shielding is available. Frequently, such tests require extensive security precautions, particularly if Category II or greater quantities of SNM are involved. The assessors may instead elect to review the results of similar tests or analyses conducted by the facility to determine the capability to detect SNM in shielded or unshielded configurations.

- If any deficiencies are noted in the installation or operation of detectors, or in the implementation of search procedures, the assessors should conduct tests that exploit those deficiencies in order to determine their significance. For example, if the assessors note that an occupancy sensor is configured such that a small vehicle might exit the portal without tripping the occupancy sensor, then the assessors could design and conduct testing to determine whether a vehicle carrying SNM could exploit the situation and avoid detection. Additional testing could be conducted to determine how large a quantity could be diverted by that method, and other tests might be considered that are designed to indicate whether the SPO notes that a vehicle is attempting to drive through the portal in an unusual pattern (that is, attempting to avoid the occupancy sensor).

- If an individual detector can be defeated, that same detector should be tested again to determine whether such defeat is repeatable. Several tests of the same detector may be required to determine whether an adversary can reliably exploit a deficiency.

- If an individual SNM detector can be defeated by one or more methods (for example, walk through, pass around), then similar SNM detectors at other portals should be tested by the same method in order to determine the extent of the problem. If possible, assessors should conduct several (three to five) more tests at different portals. If most of these tests indicate the detector can be reliably defeated, there is sufficient evidence to conclude that a systemic problem exists. If no other detectors are defeated, one may conclude that an isolated deficiency was identified. If the results are inconclusive, the assessor should consider testing additional detectors. Rarely would an assessor test more than five detectors by the same method.

- If the adversary has sufficient knowledge, time, and equipment, all SNM detectors can be defeated by using sufficient quantities of shielding. Such testing should generally be conducted only if a portal is particularly vulnerable (for example, due to lack of visual searches).

Checklist

SNM Detector

Vehicle Monitor

Interview Items

Installation location: ____

____

Operational test frequency: ____

____

Operational test method: ____

____

Sensitivity test frequency: ____

____

Sensitivity test method: ____

____

False alarm history/records: ____

____

Make/model: ____

____

Tamper protection: ____

____

Tour/Visual Examination Items

Separation between detector posts? ____

____

Control settings protected? ____

____

Alarm lines buried? ____

____

Occupancy sensor? ____

____

Vehicle trap or single gate? ____

____

Visual search conducted? ____

____

One-way or two-way traffic? ____

____

Data Collection Sheet
SNM Vehicle Detector

Test Method

	Zone Tested	Operability	Sensitivity	Kick	High Background	Low Background	Occupancy Sensor	Detection	Shielded SNM	Other
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										

Comments:

SNM Detector—Hand-held

Typical Uses

- To detect SNM at MAA personnel egress points
- To detect SNM at PA personnel egress points
- To investigate anomalies at portals where walkthrough detectors are normally used
- To use as backups if walkthrough or vehicle detectors fail
- To conduct vehicle searches
- To search at vault exits
- To search at non-routine doors
- To search packages and hand-carried items.

Concerns

- Hand-held detectors can be brought very close to areas where SNM could be concealed and thus have the potential for detecting very small quantities of SNM. However, the effectiveness of the search is highly dependent on the diligence of the SPOs who conduct the searches. If the SPO does not search personnel thoroughly (back and front, both sides) or does not take sufficient time, the detection probability can be significantly reduced.

- At portals where traffic is high or when several persons exit at once, SPOs may be rushed or have difficulty controlling (separating) personnel.

- Proper operation of the detectors is essential for an effective search. SPO training is also essential to ensure that they can operate the equipment. SPOs should know how to properly orient the detector for the most effective searches. Sufficient space is necessary to properly use the detectors and to ensure continuity of operations.

- Hand-held detectors may be susceptible to tampering if not adequately controlled.

- Hand-held detectors operate on batteries and require regular maintenance.

Types of Tests

- Operability Tests

  These tests are conducted to verify proper operability. They generally involve placing SNM or other radiation sources near the detector, observing the count rate, and verifying an alarm condition.

- Sensitivity Tests

  Sensitivity tests are conducted to verify proper detection sensitivity. Such tests generally involve observing an SPO or security technician during conduct of routine acceptance tests. These tests generally involve placing a specific radiation source at a specified distance, monitoring the count rate, and verifying an alarm condition.

- Shielding or Other SNM Detection Capability Tests

  Other tests involving shielded material or SNM concealed in a vehicle or on personnel can be conducted as described in this performance test.

Test Guidelines

- Typically, the assessors conduct operability tests and sensitivity tests at a few key portals (usually two or three).

- SNM detection capability tests and shielded SNM tests should be conducted at a typical portal if an appropriate SNM source or shielding is available. Frequently, such tests require extensive security precautions, particularly if Category II or greater quantities of SNM are involved. The assessors may, instead, elect to review the results of similar tests or analyses conducted by the facility to determine the capability to detect SNM in shielded or unshielded configurations.

- If any deficiencies are noted in the installation or operation of detectors, or in the implementation of search procedures, the assessors should conduct testing to exploit those deficiencies in order to determine the significance. For example, if the assessors note that the SPOs do not usually search the backsides of personnel, the assessors could design and conduct tests to determine whether a person carrying SNM in his/her back pocket could exploit the situation and avoid detection.

- If an individual detector can be defeated or does not have proper sensitivity, that same detector should be tested again to determine whether such defeat is repeatable. Several tests of the same detector may be required to determine whether an adversary can exploit the deficiency.

- If an individual SNM detector can be defeated or does not have proper sensitivity, the similar SNM detectors at other portals should be tested by the same method in order to determine the extent of the problem. If possible, the assessors should conduct several (three to five) more tests at different portals. If most of these tests indicate that the detector can be reliably defeated, there is sufficient evidence that a systemic problem exists. If no other detectors are defeated, then one may conclude an isolated deficiency was identified. If the results are inconclusive, the assessors should consider testing additional detectors. Rarely would an assessor test more than five detectors using the same method.

- If the adversary has sufficient knowledge, time, and equipment, all SNM detectors can be defeated by using sufficient quantities of shielding. Tests should generally be conducted only if a portal is particularly vulnerable (for example, due to poorly implemented search procedures).

Checklist

SNM Detector

Hand-held

Interview Items

Location of use: ____

____

How used (backup, normal search, anomaly investigation): __________________________

____

Operational test frequency: ____

____

Operational test method: ____

____

Sensitivity test frequency: ____

____

Sensitivity test method: ____

____

Make/model: ____

____

Storage when not in use: ____

____

Tour/Visual Examination Items

Storage location? ____

____

Used according to procedure? ____

____

Means of traffic control? ____

____

Data Collection Sheet
SNM Detector – Hand-held

Test Method

	Zone Tested	Portal Location	Operability	Sensitivity	Shielding or Other SNM Detection Capability
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

Comments:

Part 3

Metal Detectors

Part 3

Metal Detectors

Objective

The objective is to test the effectiveness of metal detectors at detecting unauthorized introduction of metallic contraband, or removal of metallic SNM/shielding, through an access control portal. Although metal detectors may be used at facilities that do not possess SNM, they are primarily used at SNM facilities.

System Tested

System:	Access control system
Functional Element:	Entry and exit searches
Component(s):	Detectors (hand-held, walkthrough), including signal processing equipment and annunciation equipment; testing and maintenance of detectors

Scenario

The assessors should select one or more metal detectors for testing. The selection is based on several factors, including portal configuration and location, operating history, the number of portals, the different types of metal detectors in use (walkthrough, hand-held), and the types of locations where metal detectors are used (PAs, MAAs, others).

Assessors should observe the facility's security alarm technicians or SPOs conducting the routine operational or sensitivity testing of selected metal detectors. During this portion of the test, the assessors should observe the test procedures to determine whether the tests, calibrations, and maintenance activities are consistent with DOE orders and approved SSSPs and whether they are an effective means of testing the systems. The assessor accomplishes two goals by having the facility's security technicians conduct these routine tests. First, the facility's tests indicate the effectiveness of the test and maintenance program. The assessor can determine whether they are effective and can also have an opportunity to determine whether the selected metal detectors are properly calibrated. Second, the facility's tests should verify that the detectors are calibrated according to facility specifications to ensure that assessors will be testing a system that is operating as the facility intends. This may be important in identifying the root cause of deficiencies.

Assessors should then conduct operational and sensitivity tests, as appropriate. The purpose of these tests is to determine whether the detectors are properly calibrated and whether they are sufficiently sensitive to meet site-specific protection objectives.

The number of detectors selected for testing depends on the time available, the importance of the system in the overall protection program, and the variety of detectors used at different portals. The following guidelines are intended to assist the assessor in selecting detectors for testing:

- At very small facilities, or at facilities with only a few (that is, fewer than five PA or MAA portals), the assessors may elect to test detectors at each portal. At larger facilities, the assessors would typically select two to four portals for testing.

- Because of the configuration of the security layers, at many facilities the exit searches at the MAAs are more critical for protecting SNM than those at PAs or outer security areas. Consequently, in many cases, it is appropriate to focus efforts on the metal shielding detectors at MAA portals. However, the metal shielding detectors at PA portal exits should not normally be completely neglected.

- Entry searches at PA portals are required by DOE orders. Some facilities conduct searches at MAA exits in addition to the PA entry searches. A few facilities conduct entry searches at MAA entrances instead of at PA entrances; these entry searches require an approved exception to DOE orders. Assessors should determine where entry searches are conducted and focus their efforts on the locations that are more critical from a security perspective.

- If the first few tests do not indicate problems and there is no evidence of exploitable deficiencies, the assessors should not generally devote extensive time to testing numerous additional detectors. However, if deficiencies are apparent, the assessors should collect sufficient data (by testing additional detectors) to determine whether a deficiency is an isolated instance or there is evidence of a systemic problem. Also, if tests indicate detectors are not sufficiently sensitive to detect the goal quantity of metal, assessors may elect to repeat tests with larger items (if available) to determine the magnitude of the deficiency.

Evaluation

In order for exit searches to be effective, the metal-detection equipment must be part of an integrated system consisting of hardware, personnel, and procedures. This section deals primarily with the evaluation of the metal-detector hardware. Guidance is provided on assessing detection effectiveness and interpreting results.

The primary objective in evaluating the metal detector is to determine whether the unit effectively and reliably detects the passage of metallic weapons or specified goal quantities of shielding through the detection zone. Other points that should be considered in the evaluation include:

- Are there provisions for monitoring personnel, packages, or vehicles passing through the detection zone in order to ensure that normal procedures are followed? For example, are there provisions for ensuring that personnel:

  – Do not bypass the detector zone?

  – Do not throw items through the detection zone?

  – Do not pass through walkthrough monitors at an unusually high rate of speed (for example, run instead of walk)?

  – Pause while in walkthrough detectors?

  – Do not pass items through walkthrough monitors at an extremely slow speed?

  – Follow all site-specific procedures?

- Is the system of barriers and procedures at the portal sufficient to ensure material is not passed around the detector?

- Are the SPOs who monitor the metal detectors trained in using the equipment, and are they familiar with the search procedures?

- Are metal detector alarm response procedures clear, complete, and sufficient to ensure that all anomalies are resolved before allowing ingress or egress?

- Are provisions adequate to ensure that unauthorized personnel do not tamper with the metal detection equipment and do not have access to control settings?

- Are testing and maintenance procedures sufficient to ensure that the metal detectors are reliable and correctly calibrated?

Interpreting Results

The following guidelines are provided to assist the assessors in interpreting results in the context of system performance.

- Testing that indicates that the metal detectors can be bypassed or do not reliably detect the passage of metallic weapons or the goal quantity of metallic shielding is evidence of a potentially serious deficiency. The significance of such deficiencies must be analyzed in the context of site-specific protection objectives and the effectiveness of other complementary systems. In general, deficiencies in metal-shielding detectors (at exits) at an MAA portal are most significant at facilities that have Category I or II quantities of SNM in portable forms and that rely on a single layer of exit search. Deficiencies in metal detectors used to detect contraband (at entrances) lead to the potential for adversaries to bring weapons into a security area. Potential factors that may partially mitigate deficiencies in metal-detection equipment are additional layers of exit searches (for example, at the MAA and PA); material controls that provide high assurance that material is not diverted; and SNM in forms (that is, large pieces or irradiated) less likely to be successfully diverted.

- Testing that indicates a slight miscalibration or detector drift is significant but much less serious than gross miscalibrations or exploitable deficiencies. For example, tests may indicate the goal quantity of shielding material (for example, 100 grams of aluminum) could be passed through the detector at shoe level eight out of ten tries at one facility portal. Additional tests may indicate that a slightly larger test quantity (for example, 150 grams of aluminum) could be reliably detected (for example, ten out of ten passes). Such results would indicate a miscalibrated sensor, but not necessarily a serious vulnerability. However, these results may indicate a testing and maintenance deficiency, and assessors should consider conducting additional tests to determine whether the miscalibration is an isolated case or a systemic problem.

Special Considerations

If the assessors use test weapons or items provided by the facility, the facility point of contact should be contacted early in the planning process to determine what types and sizes of metal objects or test weapons are available.

Related tests and activities, such as SNM detector tests and reviews of portal barriers and procedures, are typically conducted concurrently with metal-detector tests.

Responsibilities

Assessors: Select the portals and detectors. Direct testing and monitor alarm annunciation.

Facility: Conduct routine tests. Provide test sources. Assign SPOs to provide security during tests, as required. Provide security technicians to conduct testing at the direction of the assessors.

Internal Coordination

Testing should be scheduled to avoid conflicts with other tests involving the protective force. Tests of metal shielding detectors should be coordinated with the MC&A topic team (if any) to avoid duplication of effort.

Security Considerations

All normal security considerations should be observed. Normally, a protective force representative must monitor tests to ensure that security is maintained.

Personnel Assignments

Test Director:

Facility Alarm System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel

- Protective force representative
- Alarm technicians.

Equipment

- Test weapons (disabled)
- Shielding material simulator, ferrous and non-ferrous.

Safety

- Follow normal operating procedures.
- Complete a safety plan.
- Notify the CAS and other alarm monitoring stations before any testing.
- Station one assessor in the CAS.
- Coordinate to prevent any undesired armed response from protective force.

Definitions

Detection zone is the volume at which the detectors are designed to effectively detect metal. For walkthrough detectors, this is the area between the detectors. For hand-held detectors, this is the area exposed to the detector during the search procedures.

Goal quantity is the quantity of metal that is to be reliably detected when passed through the detection zone and may be defined on a site-specific basis with DOE field element approval. Standard quantities should be considered to be 100 grams of ferrous or non-ferrous metal for shielding, and 200 grams of ferrous or non-ferrous metal for weapons. These quantities should be used as a goal quantity unless the facility has identified, justified, and documented an alternative goal quantity in an approved SSSP.

Metal Detector—Walkthrough

Typical Uses

- To detect SNM/shielding on personnel at MAA or PA personnel egress points (in conjunction with SNM detectors)

- To detect metallic weapons on personnel at PA (and possibly MAA) personnel ingress points.

Types

- Pulsed field
- Continuous wave.

Concerns

- Commercial metal detectors detect only moving metal. Metal objects transferred through a detector very slowly may not be detected. For effective searches, procedures must be in place to monitor personnel passing through the detection zone to ensure that no unusual activity occurs (such as very slow movement).

- Many facilities require workers to wear safety shoes that are generally steel-toed. These steel-toed shoes are a common source of nuisance alarms. Some facilities will desensitize their detectors at shoe level; however, this practice is unacceptable from a security perspective.

- The sensitivity of metal detectors can be impacted by nearby metal structures, such as swinging metal doors or metal in walls or floors. Typically, metal detectors should be located three or more feet away from massive metal structures.

- The sensitivity of metal detectors is not uniform. The position of the metal object in the detection volume and the orientation of the object can greatly affect detection sensitivity. Test procedures should test detection capability for a variety of locations and orientations.

- Metal detectors that are calibrated to detect 100 grams of non-ferrous metal are extremely sensitive and are likely to alarm when a wide variety of common objects (belt buckles, eyeglasses, coins) are passed through or when nearby metal objects are moved (for example, a swinging door). To operate effectively, high-sensitivity detectors must be located carefully (away from metal structures and, perhaps, away from other screening equipment such as x-ray units and monitors), provided with surge-free electric power, and maintained in a temperature-controlled environment. Also, provisions must be made to examine hand-carried or personal items.

- To ensure effective searches, provisions must be made for searching personnel who set off metal detectors with metal surgical implants or metal dental work.

- Detectors, wiring, and electronics may be susceptible to tampering if they are not adequately protected by methods such as buried lines, locked control panels, or tamper alarms.

Types of Tests

- Operability Tests

  These tests are conducted to verify proper operability of the detector. They simply involve walking through the detection zone with a metal object (weapon, test object, or goal quantity of shielding). Such tests should be conducted with the source placed near the left edge, center, and right edge of the detection zone and at different elevations (for example, shoe level, waist level, head level).

- Sensitivity Tests

  Sensitivity tests are conducted to determine whether the detector is correctly calibrated. Such testing generally involves observing a security technician during conduct of the acceptance test that would normally be conducted after a calibration. This may involve a series of walkthroughs designed to demonstrate that the detector has an acceptable detection probability.

- Occupancy Sensor Tests

  Although not common, some metal detectors use occupancy sensors to detect the presence of personnel in order to reduce false alarms. The sensors may be photoelectric, ultrasonic, microwave, infrared, and pressure sensitive. Occupancy sensors are tested to verify sensor operability. Generally, the facility's or manufacturer's test procedures are followed and typically involve entering the detection zone and verifying the alarm.

- Metal Detection Capability Tests

  Assessors may elect to conduct additional testing of detection sensitivity, focusing on the capability of the detectors to detect passage of metal. Such testing may involve using weapons or goal quantities of shielding and testing the detection capability with the metal concealed at various locations on the body or in packages. The assessors should use their knowledge of metal detectors, occupancy detectors, and search procedures to conduct testing to challenge the system. For example, assessors can attempt to pass material through the walkthrough monitor while avoiding the occupancy sensor. Another example is a kick test, which involves placing the weapon/shielding at shoe level and swinging the foot through the detector as fast as possible when walking through (minimizing the time in the detection zone). Tests should be conducted with a disabled weapon or quantity of shielding equal to or greater than the goal quantity.

Test Guidelines

- Typically, the assessors would conduct operability tests, sensitivity tests, and other appropriate tests (such as kick tests) at a few key portals (usually two or three). If the facility has a large number of portals and those portals use several different types of detectors or substantially different search procedures, then the assessors may choose to test one of each major type of portal detector.

- If any deficiencies are noted in the installation or operation of detectors, or in the implementation of search procedures, the assessors should conduct tests that exploit those deficiencies in order to determine their significance. For example, if the assessors note a walkthrough metal detector is not adequately monitored by SPOs, the assessors could design and conduct testing to determine whether a person could throw a weapon/shield through the detector in an attempt to avoid detection. Additional tests could be conducted to determine how large a quantity could be diverted using this method. Other tests might be considered that are designed to indicate whether the SPO notes any unusual behavior (for example, throwing items through the detector).

- If an individual detector can be defeated, that same detector should be tested again to determine whether such defeat can be repeated. Several tests of the same detector may be required to determine whether a deficiency or given means of defeat can be reliably exploited by an adversary.

- If an individual metal detector can be defeated by one or more methods (for example, walk through, pass around), the similar metal detectors at other portals should be tested by the same method of defeat in order to determine the extent of the problem. If possible, assessors should conduct several (three to five) more tests at different portals. If most of these tests indicate the detector can be reliably defeated, there is sufficient evidence of a systemic problem. If no other detectors are defeated, then one may conclude that an isolated deficiency was identified. If the results are inconclusive, the assessor should consider testing additional detectors. Rarely would an assessor test more than five detectors by the same method.

Checklist

Metal Detector

Walkthrough

Interview Items

Installation location: ____

____

Operational test frequency: ____

____

Operational test method: ____

____

Sensitivity test frequency: ____

____

Sensitivity test method: ____

____

False alarm history/records: ____

____

Make/model: ____

____

Tamper protection: ____

____

Provisions for personnel with medical/dental implants that cause alarms: _____________________

____

Provisions for searching SPOs: ____

____

Tour/Visual Examination Items

Control settings protected? ____

____

Occupancy sensor? ____

____

SPO monitoring method (CCTV, direct)? ____

____

One-way or two-way traffic? ____

____

Metal detector used to detect shielding? ____

____

Package search method? ____

____

Data Collection Sheet
Metal Detector – Walkthrough

Test Method

	Zone Tested	Portal Location	Operability	Sensitivity	Occupancy Sensor	Detection Capability	Kick	Other
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
Comments:								

Metal Detector—Hand-held

Typical Uses

- To detect SNM/shielding on personnel at MAA or PA personnel ingress points (in conjunction with SNM detectors)
- To detect metallic weapons on personnel at PA personnel ingress points
- To investigate anomalies at portals where walkthrough detectors are normally used
- To serve as backups if walkthrough detectors should fail
- To search at vault exits
- To search at non-routine doors
- To search packages and hand-carried items.

Concerns

- Hand-held detectors can be brought very close to areas where metal could be concealed and thus have the potential for detecting very small quantities of metal. However, the effectiveness of the searches is highly dependent on the diligence of the SPOs who conduct them. If the SPO does not search personnel thoroughly (back and front, both sides) or does not take sufficient time, the detection probability can be reduced significantly.
- At portals where traffic is high or when several persons exit in rapid succession, SPOs may be rushed or have difficulty controlling (separating) personnel.
- Proper operation of the detectors by the SPOs is essential for an effective search. Training is also essential to ensure that SPOs can operate the equipment. SPOs should know how to properly position the detector for the most effective searches. Sufficient space that is free of metal, such as rebar in floors or walls, is necessary to properly use the detector and to ensure continuity of operations.
- Hand-held detectors may be susceptible to tampering if not adequately controlled.
- Hand-held detectors operate on batteries and require regular maintenance.

Types of Tests

- Operability Tests

  These tests are conducted to verify proper operability of the detector. They generally involve placing metal near the detector, listening to the detector signal, and verifying an alarm condition.

- Sensitivity Adjustment Tests

  Sensitivity adjustment tests are conducted to verify proper detection capability and the SPO's or technician's ability to adjust the detector's sensitivity. Such tests generally involve observing an SPO or technician during

performance of routine adjustments. These generally entail placing a specific metal object at a specified distance, listening to the detector signal, and verifying an alarm condition.

- Shielding or Other SNM Capability Tests

  Other tests involving shielding material or weapons concealed in a package or on personnel can be conducted as described in this performance test.

Test Guidelines

- Typically, the assessors conduct operability tests and sensitivity tests at a few key portals (usually two or three).

- If any deficiencies are noted in detector operation or in implementation of search procedures, the assessors should conduct testing to exploit those deficiencies in order to determine their significance/extent. For example, if the assessors note that the SPOs do not usually search the backside of personnel, the assessors could design testing to determine whether a person carrying a weapon in his/her back pocket could exploit the situation and avoid detection.

- If an individual detector can be defeated or does not have proper sensitivity, that same detector should be tested again to determine whether such defeat can be repeated. Several tests of the same detector may be required to determine whether a deficiency or given means of defeat can be reliably exploited by an adversary.

- If an individual metal detector can be defeated or does not have proper sensitivity, the similar metal detectors at other portals should be tested by the same method of defeat in order to determine the extent of the problem. If possible, the assessors should conduct several (three to five) more tests at different portals. If most of these tests indicate the detector can be reliably defeated, there is sufficient evidence of a systemic problem. If no other detectors are defeated, one may conclude an isolated deficiency was identified. If the results are inconclusive, the assessor should consider testing additional detectors. Rarely would an assessor test more than five detectors by the same method.

Checklist

Metal Detector

Hand-held

Interview Items

Location of use: ____

____

How used (backup, normal search, anomaly investigation): ______________________________

____

Operational test frequency: ____

____

Operational test method: ____

____

Sensitivity test frequency: ____

____

Sensitivity test method: ____

____

Make/model: ____

____

Storage when not in use: ____

____

Tour/Visual Examination Items

Storage location? ____

____

Used according to procedure? ____

____

How traffic controlled? ____

____

Data Collection Sheet
Metal Detector – Hand-held

Test Method

	Zone Tested	Portal Location	Operability	Sensitivity Adjustment	Shielding	Other
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						

Comments:

Part 4

X-ray Equipment—Package Searches

Part 4

X-ray Equipment—Package Searches

Objective

The objective is to test the effectiveness of x-ray machines as tools for searching packages or hand-carried items. The tests discussed here focus on equipment performance. However, the effectiveness of an x-ray search depends heavily on the training and attentiveness of the SPOs who operate the equipment. Other tests may be designed to focus on the effectiveness of procedural implementation, the attentiveness and training of the SPO, or combinations thereof. Such tests require detailed safety plans and are discussed elsewhere.

As per DOE orders, all hand-carried items entering a PA must be searched to prevent the introduction of weapons or contraband. However, the use of x-ray machines is not a requirement for searching hand-carried items; some facilities elect to visually search hand-carried items. X-ray machines are most commonly used at PA entrances. They are used at a few facilities for PA exit (primarily to detect shielding) or at LA entrances to detect contraband.

System Tested

System:	Access control
Functional Element:	Hand-carried item entry or exit search
Component:	X-ray machine

Scenario

Assessors should select one or more x-ray machines for testing. The selection is based on several factors, including portal configuration and location, operating history, the number of portals, the different types or models of x-ray machines in use, and the types of locations where x-ray machines are employed (for example, PAs, MAAs, LAs).

The assessors should observe the facility's security alarm technicians or SPOs as they conduct the routine operational or sensitivity tests of selected x-ray machines. During this portion of the test, the assessors should observe the procedures to determine whether the tests, calibrations, and maintenance measures are consistent with DOE orders and approved SSSPs, and whether they are an effective means of testing the systems. The assessors accomplish two goals by having the facility's security technicians conduct the routine tests before testing by assessors. First, the facility's tests indicate the effectiveness of the test and maintenance program. Second, the facility's tests should verify that the detectors are calibrated according to facility specifications to ensure that assessors will be testing a system that is operating as the facility intends. This may be important in identifying the root cause of deficiencies.

Assessors should conduct sensitivity tests using step wedges or wire gauge standards. The purpose of these tests is to determine whether the x-ray machines are properly calibrated and have sufficient penetrating power. These tests simply involve passing a step wedge through the x-ray machine and determining resolution and penetration capabilities.

The assessors may also place objects in a briefcase (which may be aluminum, leather, or other material) and observe resolution capability. Resolution capability tested by this method is somewhat subjective. One useful test procedure is to oversee an SPO who is monitoring an x-ray machine and ask what types of objects alert the SPO to visually examine the items. Also, the assessors can place an object that is opaque (such as a steel box) in a briefcase and pass it through the x-ray machine to determine whether the SPO directs the briefcase to be opened and the contents examined to verify that contraband is not concealed.

The number of x-ray machines selected for testing depends on the time available, the importance of the system in the overall protection program, and the variety of x-ray machines used at different portals. The following guidelines are intended to assist the assessor in selecting detectors for testing:

- At very small facilities, or at facilities with only a few (that is, fewer than five) x-ray machines, the assessors may choose to test all units. At larger facilities, the assessors would typically select x-ray machines at two to four portals for testing.

- Entry searches at PA portals are required by DOE orders. Some facilities conduct searches at MAA exits in addition to the PA entry searches. A few facilities conduct entry searches at MAA entrances instead of at PA entrances; this procedure requires an approved exception to DOE orders. The assessors should determine where entry searches are conducted and focus their efforts on the locations that are more critical from a security perspective.

- If the first few tests reveal no problems and there is no evidence of exploitable deficiencies, the assessors should not generally devote extensive time to testing numerous additional x-ray machines. However, if deficiencies are apparent, the assessors should collect sufficient data (by testing additional x-ray machines) to determine whether a deficiency is an isolated instance or a systemic problem.

Evaluation

For the searches to be effective, the x-ray machine must be part of an integrated system consisting of hardware, personnel, and procedures. This section deals primarily with the evaluation of the x-ray machine hardware. Guidance is provided on assessing effectiveness and interpreting results.

Assessing X-ray Machine Performance

The primary objective in evaluating an x-ray machine is to determine whether that machine is capable of imaging a 24-gauge wire and has sufficient penetrating power to clearly display objects contained in a briefcase. The following points should also be considered in the evaluation:

- Are there provisions for monitoring personnel possessing hand-carried items to ensure that normal procedures are followed? For example, are there provisions for ensuring that personnel do not bypass the search?

- Is the system of barriers and procedures at the portal sufficient to ensure that hand-carried items are not passed around the search location?

- Are the SPOs who operate the x-ray machines trained in the use of the equipment, and are they familiar with the search procedures?

- Are response procedures clear, complete, and sufficient to ensure that all anomalies are resolved before allowing ingress or egress?

- Can SPOs prevent toss-through?

- Are provisions adequate to ensure that unauthorized personnel do not tamper with the x-ray machines and do not have access to control settings?

- Are testing and maintenance procedures sufficient to ensure that the x-ray machines are reliable and correctly calibrated?

- Are personnel safety procedures documented and available, and are they consistent with the Code of Federal Regulations Part 21, Section 1020.40(c) , Cabinet X-ray Systems Requirements?

Interpreting Results

The following guidelines are provided to assist the assessors in interpreting results in the context of system performance:

- Tests that indicate the x-ray machines can be bypassed or do not have sufficient resolution capability or penetrating power are evidence of a potentially serious deficiency. The significance of such deficiencies must be analyzed in the context of site-specific protection objectives and the effectiveness of other complementary systems. Deficiencies in x-ray machines used for entry searches lead to the potential for adversaries to introduce weapons into a security area. Additional layers of searches (for example, at both the MAA and PA) may partially mitigate deficiencies in x-ray machines.

- Slightly improper calibration or lack of sensitivity is significant, but much less serious than gross errors in calibrations or exploitable deficiencies. Such results would indicate improper calibration or slight lack of resolution capability, but not necessarily a serious vulnerability. These results could indicate a potential testing and maintenance deficiency, and the assessors should consider conducting additional tests to determine whether the improper calibration is an isolated case or a systemic problem.

Special Considerations

Assessors may have access to wire standards and step wedges that may be used for performance tests. Alternatively, they may use wire standards, step wedges, or similar items provided by the facility. The assessors should contact the facility early in the planning process to determine what types of test items are readily available.

Related testing and activities, such as SNM detector tests and reviews of portal barriers and procedures, are typically conducted concurrently with x-ray machine tests to increase the efficiency of data gathering.

Responsibilities

Assessors: Select the portals and x-ray machines. Direct testing and observe resolution capability and penetration power.

Facility: Conduct routine testing. Assign SPOs to provide security during testing, as required. Provide security technicians to conduct testing at the direction of the assessors.

Internal Coordination

Testing should be scheduled to avoid conflicts with other tests involving the protective force.

Security Considerations

All normal security considerations should be observed. Normally, a protective force representative must monitor tests to ensure that security is maintained.

Personnel Assignments

Test Director:

Facility Alarm System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- Alarm technicians.

Equipment

- Wire standard
- Step wedge
- Briefcase (aluminum)
- Briefcase (leather, vinyl, or other non-metal material).

Safety

- Follow normal operating procedures.
- Complete a safety plan.
- Notify the CAS and other alarm monitoring stations before any tests are conducted.
- Continue to prevent any undesirable armed response to alarms by the protective force.

Data Collection Sheet
X-ray Equipment

Test Method

	Zone Tested	Portal Location	Operability	Sensitivity	Other
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
Comments:					

Appendix C: Communications Equipment Performance Tests

Part 1

Radio Equipment

Part 1

Radio Equipment

Objective

The objective is to test the operation of radio equipment.

System Tested

System:	Communications equipment
Functional Element:	Radio communication capability
Component(s):	Base, mobile, and hand-held protective force radios

Scenario

Radio equipment is tested by listening to radio transmissions. The purpose of these tests is to verify equipment operability and transmission quality.

One method of testing radio equipment is to station an assessor at the central alarm station (CAS) or the secondary alarm station (SAS). The assessor then directs the CAS operator (after first obtaining approval from an appropriate security manager) to contact each security post (including fixed posts, mobile posts, vehicle patrols, or foot patrols) and local law-enforcement agencies (if applicable). These tests do not normally take much time and are generally conducted while the assessors are in the CAS for other reasons, such as alarm system testing.

A second method of testing radio equipment is to conduct testing from the security police officer (SPO) posts or other locations where SPOs are stationed or on patrol. With this method, the assessor instructs the SPO (after first obtaining approval from an appropriate security manager) to contact the CAS, SAS, or another post. The assessor then moves on to the next post or to a different location and repeats the procedure. Testing of radio equipment takes very little time and is normally performed during tours or testing of other equipment.

The assessors may choose to use a combination of the two testing methods to provide a more comprehensive assessment of the reliability of radio equipment.

The assessors may also elect to test the range and reliability of the radio equipment. Such tests may involve having SPOs on patrol routes attempt to contact the CAS, SAS, or other posts while at extreme ranges from those locations. Testing can also be conducted from areas where the SPOs would normally patrol, but where the transmission is shielded, such as inside or behind buildings (in particular, buildings with metal or reinforced concrete walls). If feasible, testing should be conducted during a range of weather conditions.

Evaluation

The primary objective in the evaluation is to determine whether the radio transmissions are clear and the radios are operable. The following points should also be considered in the evaluation:

- Are there alternative means of contacting the CAS or SAS in a timely manner if the radios are inoperable or jammed (e.g., telephone, intercom, beeper)? What are those procedures? Can officers determine and detect jamming?

- Does the SAS have all the radio communications capabilities of the CAS?

Special Considerations

Radio equipment tests are straightforward and usually require very little time or effort. They are normally conducted in conjunction with tours or other tests to maximize the efficiency of data gathering. Also, testing of radio equipment is usually conducted concurrently to further increase efficiency.

Special response team (SRT) radios should be tested in both clear and voice privacy/encrypted modes.

Although protective force management has taken action in recent years to provide encrypted radios for their SRT personnel, several problems have been observed by the U.S. Department of Energy Office of Enterprise Assessments. Some protective force organizations have been slow to develop procedures to install the encryption codes. Others have not established clear procedures for switching to the secure mode when necessary, or procedures for communicating between the SRT in the secure mode and the rest of the protective force in the clear mode. Also, when radios are used in the encrypted mode, range is sometimes decreased, and procedures may not always account for this change.

Responsibilities

Assessors: Select the posts and radios that will be tested, the test methods, and the time(s) of testing. Select the equipment to be tested and provide instructions to the SPOs and CAS/SAS operators after obtaining permission from appropriate managers.

Facility: Address safety concerns and ensure that protective force supervision is available to control any response.

Internal Coordination

Any indications that the radios are an unreliable means of communication may be of interest to the protective force topic team (as it relates to equipment and duties). Testing should be scheduled to avoid interference with other tests involving the protective force.

Security Considerations

Follow all normal security procedures.

Personnel Assignments

Test Director:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

A protective force supervisor should be available to control activities at the CAS/SAS or at each portal test location.

Safety:

- Follow normal operating procedures.

Data Collection Sheet
Radio Equipment

Test Method

	Zone Tested	Zone Number	Equipment Type	System Test (CAS-POST)	System Test (POST-POST)	Quality of Transmission
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
Comments:						

Part 2

Duress Alarms

Part 2

Duress Alarms

Objective

The objective is to test the operation of duress alarms.

System Tested

System:	Communications equipment
Functional Element:	Communication capability in duress situations
Component(s):	Duress switches, transmitters, and annunciators

Scenario

Duress alarm operation is tested by activating a duress switch (typically either a pushbutton for hardwired systems or a knob on a security radio) and verifying that an alarm condition annunciates in the appropriate locations. The purpose of these tests is to verify equipment operability. Other tests may be conducted that are designed to allow the assessors to observe a protective force response to a duress condition; however, such testing requires detailed planning to ensure safety, and is not discussed in this section of the assessment guide. Measures must be taken to ensure that all appropriate personnel are aware that the duress alarm condition is occurring as part of an equipment test and that no response action should be initiated.

One method of testing duress alarms is to station an assessor at a location where most or all duress alarms annunciate, such as the CAS or the SAS. The assessors then direct the CAS operator (after first obtaining approval from an appropriate security manager) to contact each security post that is equipped with a duress alarm or a duress feature on the security radio (including fixed posts, mobile posts, vehicle patrols, or foot patrols). The CAS operator instructs the SPO at each post (one post at a time) to activate his duress alarm, and the assessor then verifies the alarm conditions. These tests do not normally take much time and are generally conducted while the assessors are in the CAS for other reasons, such as alarm system testing.

A second method of testing duress alarms is to conduct tests from SPO posts or other duress switch locations. With this method, the assessor instructs the SPO (after first obtaining approval from an appropriate security manager) to activate the duress switch and verify the alarm condition at the receiving location (for example, the CAS) by telephone or radio. The assessor can test some or all of the duress alarms at that post (once at a given post, however, he should test all duress alarms there). The assessor then moves on to the next post and repeats the procedure. The advantage to this testing method is that the assessors have an opportunity to observe the location of the duress switch (that is, whether it is in a concealed location) and the SPO's familiarity with the duress alarm operation. Tests of duress alarms conducted at SPO posts take very little time and are normally performed during tours or tests of portal access control and search equipment. Normally, radios and other communications equipment are tested simultaneously with duress alarms.

The assessors may choose to combine the two testing methods for a more comprehensive assessment of the reliability of duress alarms.

Duress alarms that rely on radio frequency (RF) transmissions tend to be less reliable than hardwired systems. Tests of RF duress alarms should be emphasized, particularly in cases where an RF duress switch is located in a post situated within a building that shields RF transmissions (for example, a building with metal or reinforced concrete walls). At facilities having vehicle-based or hand-held radios with duress features, assessors may elect to test the range and reliability of the duress capability. Such testing may involve having SPOs on patrol routes activate a duress switch while at extreme ranges from the receivers. Testing can also be conducted at areas where the SPOs would normally patrol but where RF transmissions are shielded, such as inside or behind buildings.

Evaluation

The primary objective in the evaluation is to determine whether the duress alarms function as designed. The following points should also be considered in the evaluation:

- Was the SPO familiar with the location and operation of the duress switch?
- Are the duress switches located in an unobtrusive location (that is, reducing the likelihood that an adversary would notice that a duress alarm was activated)?
- Are there alternative means of alerting the CAS to a duress condition if the primary duress switch at a post cannot be activated (for example, through a duress feature on a radio, or by code words)?
- Can a duress alarm be activated in a timely fashion – either in or out of the carrying case? (Many SPOs must remove the radio from the belt holder or unbuckle the strap, then search for the button.)
- Does the primary duress annunciation station (usually the CAS) have a backup for receiving a duress condition if the primary annunciation station is compromised?
- Does the primary duress annunciation station have a duress capability that annunciates in a second location, but does not alert an adversary in the primary location?

Special Considerations

Duress alarm tests are straightforward and usually require very little time or effort. They are normally conducted in conjunction with tours or other tests to maximize the efficiency of data gathering. Also, testing of radio equipment is usually conducted concurrently to further increase efficiency.

Responsibilities

Assessors: Select the duress alarm and posts to be tested, the test methods, and the time(s) of testing. Select and provide instructions to the SPOs and CAS/SAS operators after obtaining permission from appropriate managers.

Facility: Address safety concerns and ensure that protective force supervision is available to control any response.

Internal Coordination

Any indications that SPOs are unfamiliar with duress alarm operation or locations of duress switches may be of interest to the protective force topic team (as it relates to training and duties).

Tests should be scheduled so as not to interfere with other tests involving the protective force.

Security Considerations

Follow all normal security procedures.

Personnel Assignments

Test Director:

Facility Trusted Agent:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

A protective force supervisor should be available to control activities at the CAS/SAS or at each portal where a test is conducted.

Safety:

- Follow normal operating procedures.
- Notify all locations of alarm annunciation that a test is being conducted and no response is to be initiated.
- Any SPO responses must be controlled by protective force supervision.
- Complete a safety plan.

Data Collection Sheet
Duress Alarms

Test Method

	Zone Tested	Zone Number	Alarm Type	(CAS-POST)	(POST-POST)	Alternate Means	Special Features
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							

Comments:

Appendix D: Support System Performance Tests

Part 1

Auxiliary Power Supplies

Part 1

Auxiliary Power Supplies

Objective

The objective is to test the effectiveness of auxiliary power supplies to maintain power for continuous operation of critical physical security system components.

System Tested

System: Auxiliary power supplies

Functional Element: Support functions

Component(s): Uninterruptible power supplies (UPS), engine-driven generators, fuel supplies, batteries, inverters, switches, and interfaces with other security system components, such as central/secondary alarm station (CAS/SAS), security lighting, communications, access controls, and intrusion detection system (IDS); testing and maintenance of auxiliary power supplies

Scenario

The assessors should select various sources of auxiliary power for testing. These may include a central battery-powered UPS, remotely located individual battery backups for various security system components and equipment, and one or more diesel or gasoline engine-driven generators. At least one of each type of auxiliary power source should be tested. In deciding which tests to conduct, the assessors should first determine the configuration and location of auxiliary power sources and the systems and devices (CAS/SAS equipment, radio base stations, IDS, access control system, perimeter lighting) powered by each.

The assessors should observe, if possible, the conduct of routine operational or test activities performed by electrical technicians. Maintenance, replacement, refueling, test, and operational history records should be reviewed to determine whether they are consistent with the manufacturer's recommendations and the requirements of U.S. Department of Energy (DOE) orders and approved Site Safeguards and Security Plans (SSSPs).

To the extent possible, the assessors should conduct actual auxiliary power loss tests that require automatic startup and full-load testing of all auxiliary power sources. If this is not possible because of safety or security concerns (for example, the total loss of security systems or lighting without adequate compensatory measures), simulations may be substituted. Regardless of the tests conducted, assessors should verify that auxiliary power sources automatically carry the required electrical loads until normal power is restored.

Assessors should monitor power supply testing at the CAS or SAS to verify that power switchover is properly initiated and that all security systems continue to function as required.

The following guidelines are intended to assist the assessor in conducting appropriate tests:

- At least one of each type of auxiliary power source (central UPS, individual battery packs for sensors, and engine generators) should be tested.

- Fuel supplies should be checked for diesel or gasoline engine-driven generators to ensure the adequacy of fuel quantities and the quality of the fuel. Actual fuel testing for quality is not required if facility records indicate it is performed periodically.

- If possible, testing should include actual emergency loss of normal alternating current (AC) power, automatic switchover to auxiliary power, and demonstration that power sources can assume the full electrical load required.

- Only a representative number of individual battery power supplies should be tested. Additional testing is required only if deficiencies in the tested battery supplies are evident and indicative of a systemic weakness.

Evaluation

Emergency backup power is required to ensure continuous operation of critical security systems.

Assessing Systems

The principal objective in evaluating auxiliary power supplies is to determine whether they are adequate to power all critical equipment until normal AC power is restored.

The following factors should also be considered in the evaluation:

- Do all IDS components have an auxiliary power source, with automatic switchover upon loss of primary power, that permits continuous uninterrupted operation?

- Is the failure of either primary power or emergency backup power supplies annunciated at the CAS/SAS?

- For batteries, is a low-voltage (voltage drop of 20 percent below rated power) signal annunciated at the CAS/SAS?

- Are power supplies (and fuel) adequate to operate under full load for at least eight hours?

- Are environmental control systems and venting adequate to ensure safe and reliable operation of batteries and engine-driven generators? Battery power is reduced as temperature decreases, and evaporation of electrolyte solution increases with temperature, as does the hazard of explosion.

- Are auxiliary power sources and fuel supplies protected adequately to ensure their availability for continuous reliable operation?

Interpreting Results

The following guidelines are provided to assist assessors in interpreting results in the context of overall system performance:

- Security system operation requires a continuous, reliable power supply. Testing should verify that all critical security system components have a backup power source. This should include IDS equipment, closed circuit television (CCTV), access controls, fixed base station communications equipment, all alarm annunciation equipment in the CAS/SAS, and security lighting.

- Failure of individual power supplies (other than central UPS battery supplies and generators) may indicate either an isolated failure or a systemic weakness in the maintenance and test program.

- If "load shedding" is required because auxiliary power sources are unable to instantaneously accept the full load of security equipment (for example, diesel generators require a run-up period and sequential electrical loading), the rationale for sequencing of the load should be assessed. The most critical loads (for example, alarm systems and communications) should be picked up first, followed by the less critical systems/components (for example, CCTV systems and security lighting).

- When assessing battery supplies, it is important to remember that many batteries have a predictable useful life, after which rapid degradation followed by failure can be expected. If all batteries were installed at the same time, they will likely fail in rapid succession throughout the system.

Special Considerations

Auxiliary power supply configurations vary widely depending upon the system equipment and manufacturer. Fully understanding system configuration and the manufacturer's test procedures before conducting tests is important. Test activities should not result in failure of, or damage to, critical security systems or equipment if the auxiliary power supply performs properly.

Battery power supplies may pose health and safety hazards from caustic solutions and vapors, and the potential for explosion. All safety precautions should be carefully observed.

Responsibilities

Assessors: Select power sources and fuel supplies for testing. Direct tests and monitor system annunciations and performance. Typically, one assessor will be stationed at the CAS and at least one with the test team.

Facility: Conduct routine tests/maintenance. Provide technicians and test devices as necessary. Provide radios for two-way communication. Provide security compensatory measures, as required. Provide safety equipment/clothing as required (for example, protective eyewear).

Internal Coordination

Testing should be scheduled to avoid disrupting other security system tests. If loss of perimeter lighting will result from testing, loss-of-power testing should be conducted during daylight hours. However, this presents an opportunity to evaluate restrike times for perimeter lighting and should be carefully coordinated with site personnel before testing.

Security Considerations

Follow all normal security procedures.

Personnel Assignments

Test Director:

Facility CCTV System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- Technicians
- Testers.

Equipment:

- Radio
- Protective equipment/clothing, as required.

Safety:

- Follow normal operating procedures.
- Complete a safety plan.
- Notify the CAS/SAS before conducting any test that will affect security system operation.

Auxiliary Power Supplies Testing

System Description: Central and remotely located battery UPS, gasoline/engine generators, inverters/switching devices, battery chargers, and fuel supplies

Capabilities: Provide a minimum eight-hour power supply for all critical security system equipment with automatic switchover and annunciation upon loss of primary power

Vulnerabilities: Temperature extremes, battery aging, contaminated fuel supplies, tampering

Concerns

- Batteries require routine servicing and testing to ensure proper charging, electrolyte levels, and corrosion removal. Failure to service batteries or replace them at the end of useful life can degrade operation under emergency conditions.

- Batteries pose health and explosion hazards and should be located in a fire-resistant, environmentally controlled location that avoids high and low temperature extremes, which can increase explosion potential and reduce available power, respectively.

- Generators, batteries, inverters, power switches/busses, and fuel supplies should be protected to preclude tampering. Exterior fuel tanks and filler points are especially vulnerable.

- Power ratings on batteries and generators can sometimes be misleading. For example, in the case of batteries, below-freezing temperatures can reduce available power by more than 50 percent. Generators may be unable to instantaneously carry the full rated load, especially if the electrical drive shaft is not of the continuously turning type driven by an auxiliary electric motor.

Types of Testing

- Full Loss-of-Power Test

  If possible, without unacceptable security system degradation, a test should be performed where all primary (commercial AC) power is disconnected from all security system components. The purpose of this test is to ensure that all system power loads can be handled, usually by the UPS batteries and then by the emergency generators. The loss-of-power test should last at least ten minutes, and preferably one hour, to adequately demonstrate system reliability. Proper functioning of all security system equipment (including lighting) should be verified, as well as proper annunciation of all power supply status indicators in the CAS/SAS.

- Remote Power Supply Tests

  If remotely located power sources are used, a representative sample should be assessed and tested. Generally, there will be battery packs for intrusion detection sensors, sensor control units, or communications equipment. The test usually consists of removing the primary power lead to the device and verifying that the device continues to operate on battery power and that a status indication is received by the CAS/SAS.

- Power Status Indication Test

  As part of the loss-of-power and remote power supply testing, annunciation of the status of all power sources at the CAS/SAS should be verified. The annunciation should indicate which source of power is being used

and the status of the primary AC power source, any battery backups, and the emergency generators. This test involves the simulation of reduced output and requires assistance from facility electrical technicians.

Test Guidelines

- The foregoing testing should usually be conducted during daylight hours for safety and security reasons. If loss-of-power testing will affect perimeter security lighting, testing should include turning on all lighting or arranging for special compensatory measures for testing during periods of darkness.

- At least one of each type of auxiliary power supply should be tested.

Checklist

Auxiliary Power Supplies

Interview Items

Types of power supplies in use: ____

____

Makes/models: ____

____

Where located/how protected: ____

____

Systems connected to each type power supply: ____

____

Operational test frequency: ____

____

Environmental protection equipment: ____

____

Physical protection measures: ____

____

Fuel supplies and locations: ____

____

Special equipment (status annunciators, inverters, battery chargers): ____

____

Maintenance history/records: ____

____

Power rating adequate to meet needs of all equipment (kWh or amp rating): ______________________________

____

Frequency and duration of generator operation: ____

____

Tour/Visual Examination Items

Physical protection OK? ____

____

Environmental controls (Heating, Ventilation, and Air Conditioning) OK?_____________________________

____

Fire and electrical safety OK? ____

____

Fuel supplies adequate? ____

____

Gasoline fuel replenished every six months? ____

____

Status annunciators (audible/visual) adequate? ____

____

Battery electrolyte and specific gravity OK? ____

____

Battery connections OK (no corrosion)? ____

____

Data Collection Sheet
Auxiliary Power Supply Testing

Test Method

	Zone Tested	Zone Number	Full Loss of Power	Remote Power Supply	Power Status Indication	Duration of Auxiliary Power
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						

Comments:

Part 2

Tamper Protection and Line Supervision

Part 2

Tamper Protection and Line Supervision

Objective

The objective is to test the effectiveness of components used to indicate that detection and alarm devices or transmission lines to annunciators have failed or have been subjected to tampering.

System Tested

System: Tamper protection

Functional Element: Support functions

Components: Tamper switches (contacts, magnetic switches, plungers), line supervision circuits, signal processing equipment. Testing and maintenance.

Scenario

The assessors should select tamper alarms and line supervision circuits for testing in conjunction with IDS and CCTV system testing. During site tours in preparation for IDS and CCTV testing, the assessors should look for the related tamper/line supervision components to be tested.

The assessors should select tamper-protection devices for testing based on consideration of the number, type, deployment, and operational history of the components. If facility alarm technicians are conducting tamper-protection testing or maintenance, the assessors should observe the procedures to determine whether they are consistent with DOE orders and the approved SSSPs, and whether they are effective in testing system performance. These test and maintenance activities are an indicator of maintenance program effectiveness and provide assurance that the assessors will be testing a system that is operating as the facility intends. Maintenance program effectiveness indicators may be important in identifying the root cause of deficiencies.

The assessors conduct tests by opening tamper-protected enclosures (that is, sensor covers, junction boxes, CCTV housings) and creating open and short conditions in electrical circuits to determine whether any of these actions could occur without annunciation at the CAS and SAS.

The assessors monitor tamper and failure annunciation in the CAS/SAS. They also observe the operation of related systems (such as the CCTV) and the actions of CAS/SAS operators.

The number of tamper devices and line supervision circuits tested depends on the time available, the importance of the protected system in the overall protection program, and the variation in the individual protection zones. The following guidelines are intended to assist the assessor in selecting devices and circuits for testing:

- Test at least two of each type of tamper alarm device. If more than one line supervision (failure indication) method is employed, one of each type should be tested.

- If practicable, test tamper alarms and line supervision circuits in conjunction with other tests (CCTV and IDS).

- If the first few tests do not indicate problems and there is no evidence of exploitable deficiencies, the assessors should not devote extensive time to testing numerous devices and circuits. However, if deficiencies are apparent, the assessors should collect sufficient data to determine whether a deficiency is an isolated instance or evidence of a systemic problem.

Evaluation

To ensure proper operation of the overall security system, reliable measures for detecting tampering and failure of critical security system components are necessary.

Assessing Tamper Protection

The primary objective in evaluating the tamper-protection subsystem is to determine whether it clearly annunciates equipment tampering or failure at the CAS/SAS. The following points should also be considered in the evaluations:

- Are all tamper and failure conditions indicated at the CAS/SAS in both the access and secure modes (if applicable to the protected equipment)?
- Are all junction boxes in accessible locations equipped with tamper alarms?
- Do all IDSs and emergency exit alarms have tamper indication and line supervision, indicating the type and location of the alarm?
- Are all alarm lines continuously supervised to detect open, short, or signal substitution conditions?
- Does the CCTV system have a loss-of-video signal indication for each camera?
- Do new IDSs for special nuclear material and vital equipment facilities use continuously polled digital line supervision with unique digital address codes and pseudo-random polling (or, alternatively, encryption)?

Interpreting Results

The following guidelines are provided to assist the assessors in interpreting results:

- Tests which indicate that a knowledgeable adversary could defeat tamper/supervision protection without being detected in a significant fraction of the attempts are evidence that system protection is unreliable. The significance of this finding must be analyzed in the context of the site-specific protection objectives, redundancy, and the effectiveness of other complementary systems.
- In some cases, facility tests indicate that tamper indication and line supervision function correctly, but assessor tests indicate that the protection can be defeated or does not function reliably. In such cases, the test and calibration procedures and the quality assurance program likely have deficiencies.
- Facility tests that indicate that the sensors are calibrated according to specification, in conjunction with assessor tests that confirm that the sensors are capable of reliably detecting tampering or failure, are evidence that the tested portion of the system is effective and that test and maintenance procedures are effective.

However, the limitations of the tests must be recognized. For example, not all modes of defeat (for example, signal substitution) may have been tested, and the test may not have stressed the system to the limit (for example, multiple attempts prior to system reset).

- Facility tests that indicate that one or more tamper or supervision devices are not functioning according to specifications may simply be an indicator of an isolated instance of component failure. However, such deficiencies may also be an indicator of systemic deficiencies with the test and maintenance program or the age and condition of the devices. If facility tests indicate that devices are out of calibration, the assessors should consider instructing the facility's technicians to test a representative sample to determine the extent of the problem.

Special Considerations

Tamper and line supervision tests are usually conducted in conjunction with related tests of CCTV equipment and the intrusion detection and access control systems to increase the efficiency of data gathering.

Responsibilities

Assessors: Select the tamper alarms and line supervision circuits for testing. Direct testing and monitor alarm annunciation. (Typically one assessor will be stationed at the CAS and at least one at the tested device.)

Facility: Conduct routine testing. Provide security technicians. Provide test devices as necessary. Provide security police officers to ensure security during tests, as required. Provide radios for two-way communication. Provide personnel to conduct tests at the direction of assessors.

Internal Coordination

Tests should be scheduled to avoid conflict with other tests involving the protective force.

Security Considerations

Follow all normal security procedures.

Personnel Assignments

Test Director:

Facility Alarm System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- Technicians
- Tester.

Equipment:

- Radio
- Test devices (for example, voltmeters and other electrical test devices).

Safety:

- Follow normal operating procedures.
- Complete a safety plan.
- Notify the CAS and other alarm monitoring stations before testing is conducted.
- Station one assessor in the CAS.
- Coordinate with protective force personnel to prevent any undesired armed response.

Tamper Protection/Line Supervision

System Description: Tamper sensors (magnetic switches, contact closures, plungers), line supervision signal generators and processors, end-of-line resistors, and status indication annunciators

Capabilities: Indication of physical tampering (usually opening a protected enclosure) and signal line open, short, or signal substitution condition

Vulnerabilities: Improper alignment or sticking of switches or contacts, gaps in protection, improper annunciation of status indication

Concerns

- Generally, the failure to provide complete tamper indication and line supervision for all security system elements and devices requiring protection is the most significant weakness. All critical components should be covered: intrusion sensors, sensor controls, communication devices (for example, multiplexers), transmission lines, CCTV enclosures and signal equipment, cable junction boxes, power supply cabinets, and any other critical system support equipment.

- Tamper devices (magnetic switches, plungers, closure contacts) should be inaccessible and located inside a protected space to prevent a knowledgeable adversary from defeating the device.

- Mechanical tamper devices (for example, plungers) must be serviced to ensure that they do not stick in the secured position because of rust, freezing, or accumulation of dirt.

- Indication of the status of tamper devices and line supervision should be prompt and should continue even after the device returns to a normal condition (although the status indicator may show “return to normal” by change of color). This feature precludes, for example, opening a protected enclosure and quickly taping down the contact plunger to indicate that the tamper condition has returned to normal.

- Line supervision should include the entire circuit to be protected: the protected device (for example, sensor or CCTV camera), local wiring to a control device (for example, multiplexer or control panel), the transmission medium (for example, bi-directional multiplexed cable loop or free-space transceiver), and the final signal processing and annunciation equipment (for example, CAS/SAS monitoring equipment).

- CCTV camera protection should include loss-of-signal monitoring and annunciation as part of the alarm annunciation system. Loss of the actual CCTV image on the television monitors at the CAS/SAS should not be relied upon for this function since failure of the monitor could be confused with loss-of-video signal.

- Multiple tamper devices are sometimes included on a single alarm circuit to reduce wiring and signal processing requirements. This can be a significant weakness since the actual type and location of the alarm, and the number of affected devices, may not be known from the information displayed at the alarm console.

- In the case of line supervision, the type and location of the failure may not be known from the alarm annunciation. System redundancy and the number of sensor signals that may be lost because of a single communication failure should be considered in assessing the impact of such a configuration. If a single point failure (for example, open or short condition) will affect a large number of security system devices, it is especially critical that the nature and location of the failure be clearly annunciated. Otherwise, an adversary could disable the system and gain considerable time to act while maintenance personnel attempt to locate and repair the communications failure.

- Signal lines should be protected by use of metal conduit and, whenever possible, should be buried underground. To the extent possible, interior cable runs should be located within spaces that are protected by active IDSs and should be located in inaccessible places.

- Often slow computer response will allow the assessor to open a junction box pull or push tamper switch to "Nonalarm" position. If done rapidly, no alarm will be reported in CAS or SAS.

Types of Tests

- Contact Closure Test

  This test is conducted by simply opening a protected enclosure. An alarm should be generated before gaining access to wiring inside the enclosure. The contact switch or plunger should be promptly closed by hand (or using tape). This test should verify that an initial tamper alarm was generated before physically closing the contact, and that the alarm remains after the contact was closed.

- Balanced Magnetic Switch (BMS) Test

  BMS sensors should be tested by opening the protected enclosure one inch to determine whether an alarm is generated. A hand-held magnet should then be placed against the switch housing in an attempt to simulate closure of the device. An additional step of placing a magnet against the BMS when the tamper switch is closed and active may be used to determine whether capture of the switch is possible (this test is feasible only if the magnetic switch is accessible when the enclosure is closed). This test should verify that (1) an initial tamper alarm is generated when the closure is opened or when a magnet is brought into contact with the BMS, and (2) that the alarm continues even though a hand-held magnet is used to replace the actual magnet of the switch.

- Line Supervision Test

  Line supervision tests are conducted by creating an open or short condition in the tested communication signal line. An open condition is created by disconnecting wires/cables from a terminating block or other connecting point. Ground faults are also created at these connecting points. No actual cutting of any signal lines should be performed, nor should grounding be done if damage to equipment will result. An open or short condition should be indicated by an alarm regardless of the duration of the condition. Therefore, return the open or short condition to normal as quickly as possible to verify that the line supervision was able to promptly detect the condition. This capability is important to prevent a fraudulent signal being substituted for the normal signal on the transmission line.

Test Guidelines

- Testing should be conducted in conjunction with CCTV, intrusion detection, and access control tests to maximize data-gathering efficiency.

- At least two of each type of tamper alarm device should be tested.

- At least one of each type of line supervision in use should be tested.

- No test should result in damage to equipment. Line supervision tests should not be conducted if serious disruption of critical security systems (that cannot be compensated for) will occur.

Checklist

Tamper Switches

Interview Items

Installation location: ____

____

Operational test frequency: ____

____

Operational test method: ____

____

Self-checking provisions (if applicable): ____

____

Maintenance procedures: ____

____

False/nuisance alarm history/records: ____

____

Make/model: ____

____

Type(s) used: ____

____

Systems covered: ____

____

Operational test frequency: ____

____

Operational test method: ____

____

Tour/Visual Examination Items

Cable in conduit/buried? ____

____

Tampers present? (junction boxes, sensor housings, CCTV enclosures, multiplexers, power supply cabinets)

____

____

Appendix E: Personnel and Procedure Performance Tests

Part 1

General Background

Part 1

General Background

Introduction

In addition to testing physical security equipment, the assessors may elect to design and conduct performance tests that stress the facility's security-related procedures and the personnel who perform security-related tasks.

Personnel and procedures are an essential part of an effective security program at all U.S. Department of Energy (DOE) facilities. Many DOE facilities do not have sophisticated automated security hardware and rely heavily on personnel and procedures to perform security functions such as searches and intrusion detection. Procedural controls are necessary for many aspects of security including material transfers, material surveillance, patrols, alarm response, entry control, badge issuance, and visitor control. Trained, dedicated, and alert personnel are necessary to implement procedures and interface with security equipment. At a typical facility, security-related procedures are implemented by a wide range of personnel and facility organizations, including members of safeguards and security, testing and maintenance, operations and production, personnel security departments, and management.

Although personnel and procedures are essential to a physical security system, testing the effectiveness of personnel and procedures during an assessment is often more difficult than testing equipment. When designing, conducting, and evaluating tests of personnel and procedures, the assessors must consider the following complexities:

- Procedures are site specific.
- Procedures are not always formally documented.
- Procedures are not always current.
- "Real world" implementation may vary from documented procedures.
- Effectiveness varies from person to person.
- Individual motivation and alertness levels vary.
- Security awareness is heightened during an assessment.
- Safety must not be compromised.
- The element of surprise may be difficult to simulate.
- Tests are not always repeatable; for example, a security police officer (SPO) may find a contraband item in a briefcase one time but not the next.

Because of these complexities, testing of personnel and procedures requires extensive planning. However, in many cases, these tests provide valuable information on the effectiveness of the overall system. The assessors must examine their resources and information needs and determine whether the benefits of the information gained from personnel and procedures testing is worth the resource expenditure necessary to design and conduct them, or whether resources are better spent on other activities.

Test Design, Conduct, and Evaluation

As part of the normal assessment activities, the assessors should test the security systems, including equipment and procedures. When the assessors identify a procedure critical to system effectiveness, they should consider designing a performance test to provide information on the effectiveness of that procedure. Part 2 of this appendix provides a "laundry list" of typical procedures or personnel actions that are candidates for testing. Other candidate procedures may be identified by the assessors. Once the assessors decide to conduct a test, they would generally follow the steps listed below:

- Develop a scenario.
- Determine evaluation criteria.
- Assign responsibilities.
- Arrange logistics.
- Address safety concerns.
- Develop a performance test plan.
- Coordinate with other topic teams.
- Schedule testing.
- Conduct testing.
- Evaluate results.

Scenario

A scenario is a detailed description of the activities assessors will conduct (or direct the facility to conduct). The scenario activities are designed to provide an opportunity for the assessors to observe the system response under controlled conditions. This may involve setting up a situation in which the assessors can observe whether personnel follow procedures and whether the objective of a procedure is achieved (for example, detect a weapon in a visual search of a briefcase). Sample scenarios are included in Part 3 of this appendix. The scenarios in Part 3 are not intended to be a comprehensive set, but rather are intended to guide assessors in developing site-specific scenarios.

Developing scenarios usually requires the involvement of a facility representative to act as a trusted agent. The trusted agent helps the assessors design the tests and arrange logistics while maintaining confidentiality so the test is not compromised.

Where necessary, the scenario should include provisions for repeating a test with different persons or at a different location in order to provide sufficient data to draw valid conclusions. For example, a test involving a weapon in a briefcase might be conducted at three different locations. If one SPO fails to conduct a thorough search and misses the item, the facility may argue that it was a random occurrence. However, if three SPOs do not conduct thorough searches, then the assessors may conclude that procedures are not diligently implemented and that there is a systemic problem.

Evaluation Criteria

The assessors should thoroughly understand what to expect during a test and what the site-specific objectives are for the tested element. The assessor should document the evaluation criteria in the performance test plan. The evaluation criteria must be consistent with DOE orders.

Responsibilities

The responsibilities for conducting these tests should be clearly defined. This includes identifying the field element's responsibilities as well as those of each assessor.

Logistics

The assessors should carefully coordinate all logistical aspects of the tests. The following items should be considered:

- The need for equipment, test sources, and standards
- The need for special personnel, such as health physics technicians, to conduct various steps of the test
- Any requirements related to operating conditions (for example, day or night, access or secure mode)
- The need for additional security measures.

If observers (other than the persons involved in the test) are necessary, arrangements should be made to station them where they will not interfere with the test or confuse or otherwise influence the personnel being tested.

Safety Concerns

Testing should be conducted with the highest regard for safety. The assessors should be certain that adequate measures are implemented for ensuring that:

- Armed response is prevented or controlled.
- Exposure to radioactive or toxic material is avoided or minimized.
- Facility, DOE, and other safety procedures are strictly followed.
- The assessors and facility have adequate means to interrupt or cancel the test if safety is compromised, or if an actual safety or security situation arises during the test.

Performance Test Plan

Performance test plans should be developed and included in the assessment plan. The performance test plan should be sufficiently detailed so that a reviewer would understand the basic scenario and evaluation criteria. Safety measures should also be included, and responsibilities should be defined.

Coordination

The assessors should coordinate with other topic teams before conducting testing to avoid overlapping or conflicting activities. Other topic teams may be interested in the test results and may assist with the testing or send observers. The teams should ensure that tests that may conflict with each other are not scheduled simultaneously. For example, testing the response to an intrusion alarm may result in facility lockdown, which could interfere with other tests.

Scheduling

Testing should be scheduled in advance, allowing time for management review, coordination, and safety reviews. Information related to tests that rely on "surprise" (for example, tests for detecting contraband in a briefcase or an alarm response test) should be carefully controlled to decrease the likelihood of compromising the test.

Some tests need to be conducted under certain operational conditions (for example, night shift). These tests should be conducted as realistically as possible.

Some tests may have to be repeated several times or in more than one location to provide sufficient data for evaluation purposes. Such testing should be scheduled accordingly, with consideration given to the likelihood that the "word" will spread quickly when a test is conducted and that subsequent results may be biased.

Conduct

The test should be conducted according to the test plan, with as little deviation as possible. If any deviation is necessary, the assessors, in conjunction with the facility representatives, should verify that safety is not compromised and that the objectives of the test are still valid. The assessors should be prepared to interrupt or cancel the test whenever a safety concern is identified and should have a means of promptly notifying all personnel when such an action is deemed necessary.

Evaluation

Performance test results are evaluated against DOE orders and site-specific requirements. Performance tests are not individually rated. Instead, the information gathered in the test is factored in with other information collected during interviews, other tests, and document reviews, and the overall effectiveness of the system is evaluated.

Part 2

Candidate Procedures

Part 2

Candidate Procedures

Introduction

This section lists the procedures and personnel actions that are candidates for performance testing by the physical security systems assessment team. Assessors may identify other procedures that are suitable for testing during the site-specific reviews.

Entry Control Systems

General

- Procedures to verify access authorization by checking identifiers (for example, names and employee numbers) against an access authorization list (hard copy or computer file)
- Procedures to log non-routine entries (for example, visitors, personnel during off-shift, and personnel not normally assigned) at security areas
- Procedures to verify the identity of a visitor before issuing a badge/pass/credential
- Procedures to verify the authorization and clearance of a visitor before issuing a badge/pass/credential
- Procedures to verify the access authorization of vehicles.

Badge Systems

- Badge checks by SPOs at material access areas (MAAs), Protected Areas (PAs), Limited Areas (LAs), or other security areas
- Procedures to store and account for badges
- Procedures to report lost badges and notify appropriate personnel
- Badge/personnel identification checks at portals that use closed circuit television (CCTV) to verify the identity of personnel entering a security area.

Automated Systems

- Procedures to store and account for coded credential devices (for example, cards and stocks of blanks)
- Procedures to enroll personnel in an automated access control system (for example, card reader, biometric identification device)
- Procedures to delete personnel from an automated access control system
- Procedures to monitor personnel as they interface with access control equipment to ensure they follow authorized procedures.

Searches

- Use of hand-held equipment (for example, metal detectors) to search personnel entering a security area.
- Use of hand-held equipment, such as metal or special nuclear material (SNM) detectors, to search personnel leaving a security area.
- Procedures to monitor personnel passing through walkthrough SNM or metal detectors.
- Use of hand-held equipment (for example, SNM detectors, mirrors) and visual examination techniques to search vehicles entering or leaving a security area.
- Procedures to search hand-carried items or packages entering or leaving a security area (including visual, x-ray, or SNM detector searches).
- Procedures to search packages too large to pass through an x-ray machine.
- Procedures to search packages unsuitable for visual examination (for example, sealed components).

Barriers

General

- Procedures to patrol and inspect exterior security area perimeter barriers (for example, fences) to verify integrity and detect unauthorized objects (for example, ladders) or conditions (for example, excessive soil erosion under a fence)
- Procedures to patrol and inspect interior security area perimeters barriers (for example, MAA walls, doors, windows) to verify integrity and detect penetration
- Procedures to patrol and inspect security containers to verify they are locked/secured
- Procedures to patrol and inspect vehicle barriers to verify integrity
- Procedures to inspect activated barriers to verify integrity and detect tampering
- Procedures to lock down a facility or area in response to a security condition.

Lock and Key Controls

- Procedures to issue keys
- Procedures to store keys
- Procedures to change locks and lock cores
- Procedures to issue combinations
- Procedures to change combinations.

Intrusion Detection Systems

Electronic Intrusion Alarm Systems

- Procedures to assess intrusion alarms.

- Procedures to assess tamper and line-supervision alarms.

- Procedures to respond to alarms, including response time; also, response procedures when multiple alarms occur simultaneously.

- Procedures to record/log alarms.

- Procedures to patrol perimeters and security areas and to inspect systems to ensure that protection is not degraded (for example, verify that no ladders, scaffolds, or equipment that could be used to bridge/jump the exterior sensors are in isolation zones; verify that no equipment is blocking interior sensors).

- Compensatory procedures used during failure of an alarm system or components.

- Procedures to place alarms in access mode and return them to service mode.

Lighting

- Procedures to patrol or inspect areas and identify/correct lighting deficiencies, including burned-out bulbs
- Compensatory measures used during failure of lighting systems.

Visual Detection

- Procedures to continuously monitor perimeters or areas
- Procedures to patrol perimeters or areas.

CCTV Assessment Systems

- Procedures to assess alarms
- Procedures to track intruders using CCTV with pan-tilt-zoom features
- Procedures to periodically verify the operability of CCTV systems that are not continuously displayed (for example, call-up or sequenced monitors).

Communications Equipment

- Procedures to communicate a duress situation when the duress switch cannot be activated, such as the use of code words
- Procedures to respond to a duress condition.

Radio Systems

- Investigation/response procedures implemented if an SPO does not respond to a periodic radio check
- Procedures to switch to different frequencies during specified conditions (for example, tactical response).

Other

- Procedures to use other systems as a backup if primary system capability is lost
- Procedures to use public address systems to direct facility personnel during security situations or emergency evacuation conditions.

Testing and Maintenance

Testing

- Procedures to test security-related hardware
- Procedures to report incorrectly calibrated or inoperable equipment
- Procedures to record test results.

Calibration/Preventive Maintenance

- Procedures to maintain/calibrate security-related hardware
- Procedures to initiate repair/replacement of degraded equipment
- Procedures to record maintenance results.

Corrective Maintenance/Repair

- Procedures to isolate/locate causes of failures
- Procedures to repair/replace components
- Procedures to record repair/maintenance.

Quality Assurance

- Procedures to verify test results
- Procedures to verify proper maintenance (for example, functional tests by a second person)
- Procedures to verify work by vendors
- Procedures to inspect new components and components repaired by offsite vendors
- Procedures to verify integrity of system following software modification.

Auxiliaries and Interfaces

Protective Force Procedures

- Procedures to respond to evacuations caused by fire, criticality, or other emergency situations
- Procedures to escort SNM shipments
- Procedures to verify SNM transfer authorization
- Special post orders
- Procedures to patrol areas.

Production/Operations/Safeguards Department Procedures

- Procedures to maintain material surveillance
- Procedures to verify SNM transfer authorization
- Procedures to transfer SNM
- Procedures to verify non-SNM transfers out of an MAA
- Procedures to control SNM during/following an emergency evacuation and safety situation (fire, accident)
- Procedures to enter/secure a storage area.

Part 3

Sample Scenarios

Part 3

Sample Scenarios

Introduction

This section presents five sample scenarios for performance tests of personnel and procedures. These samples represent a wide range of test-design complexity. Assessors will also likely develop scenarios for testing other procedures. Any scenarios developed to test a site-specific procedure that are proven effective and are applicable to other facilities should be submitted to the DOE Office of Enterprise Assessments for incorporation into the appropriate assessment guide.

Scenario 1—Badge Checks

At facilities that rely on badge checks to control entry into a security area, assessors may test the effectiveness of the badge checks (in particular the alertness of the SPO) by using the following scenario:

- Arrange for a person who normally accesses a security area to attempt to gain access to that area by using a badge that has incorrect or outdated information.

- Arrange with Badge Office to obtain an "improper" badge – that is, a badge that does not meet the facility's requirements. The improper badge may be expired (if dates are included on badge), may have the right name but wrong person's picture (or vice versa), or may omit an authorization symbol specific to that area. Alternatively, the person may attempt to enter using a different person's badge.

- Have the person follow normal procedures to enter the security area, preferably during high-traffic periods or when the SPO is likely to be rushed.

- Determine whether the SPO checks the badge, detects the improper badge, denies entry to the person, and responds to the unauthorized attempt as required by local procedures.

Scenario 2—Perimeter Patrols

Facilities that have perimeter alarm systems must periodically patrol the alarmed perimeter to reduce the risk of adversaries defeating alarm systems through bridging techniques. The following scenario is one method of testing the effectiveness of patrols, in particular the alertness and training of the SPO on patrol. This scenario is particularly applicable at facilities that do not frequently monitor the perimeter with CCTV, that have relatively small isolation zones (for example, 12 feet or less from fence to fence), and that do not use fence-mounted sensors. Assessors should:

- Arrange for the facility to provide an extension ladder.

- Direct a facility representative to covertly place the extension ladder near the fence line or, if feasible, across the tops of the two fences, such that an adversary could use the ladder to crawl across the isolation zone without entering the sensor detection zone. The ladder should be placed in a location that is not visible from a protective force post, preferably after dark.

- Monitor central alarm station (CAS) operations and radio systems to determine if the protective force patrol identifies a potential security concern, whether program reporting procedures are followed, and whether appropriate response is initiated.

Scenario 3—Maintenance Personnel

The effectiveness and knowledge of maintenance personnel can be tested by the following scenario:

- Arrange with the facility to intentionally disable a security component shortly before a routine calibration. For example, a lead on one channel of an SNM walkthrough monitor could be disconnected.
- Observe maintenance team members during their routine calibration procedure, and determine whether they correctly identify the problem and initiate corrective action.

Scenario 4—Visual Detection

Facilities that rely on visual detection at a security area can be tested with the following scenario:

- Arrange for a small team (of one or two facility representatives or assessors) to dress in dark clothing.
- Plan an entry route to the facility that avoids heavy populated areas and well-lighted areas, maximizes the use of cover and concealment, and avoids direct viewing from SPO visual observation posts.
- Have the "adversary" attempt to enter the facility along the planned route.
- Determine whether the SPOs in observation posts or on patrol detect the "adversary" before gaining access to a security area.

Scenario 5—Emergency Evacuation

Facilities that have SNM must protect it during an emergency evacuation. The following scenario may be used to observe the protective force response to a simulated evacuation when the protective force procedures call for an SNM "sweep" of the area following the evacuation. Assessors should:

- Choose a convenient time, preferably causing minimal impact on operations, and when no SNM is out of secured storage (to ensure that security is not degraded by the test).
- Station an "adversary" possessing a radioactive source (non-SNM) near an MAA emergency exit.
- Direct a facility representative to simulate a criticality alarm and direct personnel to evacuate (the personnel should be informed that the alarm is a test and directed to exit at controlled speed to minimize safety concerns).
- Direct the "adversary" to exit the area as soon as the "criticality alarm" is sounded and drop the radioactive source in a location suitable for later pickup (for example, a trash can) before proceeding to his/her designated assembly point.
- Observe the protective force's response to the evacuation alarm and its procedures for controlling exiting personnel.
- Determine whether the protective force locates the radioactive source during the SNM sweep.

Part 4

Badge Checks

Part 4

Badge Checks

Objective

The objective is to test the effectiveness of the badge checks in detecting and preventing unauthorized entry attempts. Specific tests may focus on the effectiveness of procedural implementation, the tamper-resistance of the badge, the attentiveness and training of the SPOs, or combinations thereof.

System Tested

System: Access control

Functional Element: Personnel identification and verification

Component: Badge check at security area portal or security checkpoint

Scenario

Option 1—Authorized Person/Incorrect Badge

The assessors should arrange for a person who normally accesses a security area to attempt to gain access to that area by using a badge that has incorrect or outdated information.

- Arrange with the badge office to obtain an "improper" badge (that is, a badge that does not meet the facility's requirements). The improper badge may be expired (if dates are included on badge), may have the right name but wrong person's picture (or vice versa), or may omit an authorization symbol specific to that area. Alternatively, the person may attempt to enter using a different person's badge.

- Have the person follow normal procedures to enter the security area, preferably during high-traffic periods or when the SPO is likely to be rushed.

- Determine whether the SPO checks the badge as per his procedures, detects the improper badge, denies entry to the person, and responds to the unauthorized attempt as per procedures.

Option 2—Unauthorized Person/Fake Badge

The assessors should arrange for a person who is not authorized access to a security area to attempt to gain access to that area using a fake badge.

- Obtain a badge for an unauthorized person. The easiest way of doing so is to use the badge of an authorized person, preferably one who bears some physical resemblance to the person attempting entry. Alternatively, arrange with the badge office to obtain a badge, insert, or stock for the person(s) attempting entry. Depending on the specifics of the facility's operations and the test objectives, the badge may be correct in every detail or may be flawed in one or more aspects (for example, improper lamination to simulate an adversary who has tampered with the badge).

- Have the person follow normal procedures to enter the security area, preferably during high-traffic periods or when the SPO is likely to be rushed.

- Determine whether the SPO checks the badge as per procedures, detects the improper badge, denies entry to the person, and responds to the unauthorized attempt as per procedures.

Evaluation

The primary factor in the evaluation is whether the objectives of the badge check were met (that is, whether the unauthorized access attempt was detected and entry denied). The following questions should also be considered in the evaluation:

- Did the SPO correctly follow all procedures when checking the badge?

  – If holding or touching the badge is required, did the SPO do so?

  – If the badge is in a clear plastic holder and touching the badge is part of the procedure, did the SPO remove the badge from the holder?

  – If access codes are included on the badge, were they checked before entry was allowed?

  – If a badge exchange is part of the procedure, was it performed correctly?

  – Did the SPO ensure that the person attempting entry removed sunglasses or other articles in order to facilitate comparison?

- Did the SPO correctly identify discrepancies with the badge (if any), such as:

  – Wrong person's picture?
  – Wrong name?
  – Expired?
  – Wrong access code?

- If checking the name or badge number against an access list is part of the procedure, did the SPO correctly do so?
- Were applicable entry logs (if any) filled out correctly?
- If a discrepancy is detected, did the SPO deny entry and follow the appropriate response procedures such as:

  – Detain suspect?
  – Call supervisor and backup?
  – Shut down portal (if required)?
  – Other?

The specific objectives of the test should be kept in mind during the evaluation. Tests involving a normally authorized person with an incorrect badge are primarily designed to determine how attentive the SPO is and how thoroughly the badges are checked. Tests involving an unauthorized person are primarily designed to determine whether an adversary can use a fake badge to gain entry. The following factors should also be considered when evaluating the test results:

- Are there any related or complementary systems that perform the personnel identification function (for example, a card reader in conjunction with the badge check, or a requirement for an escort with every visitor)?

- Does the adversary have to pass through more than one layer in the system to gain access to security interests?

- Are controls inside the security area likely to be effective, or is the adversary essentially unrestricted once inside the area?

Special Considerations

More than one badge test should be conducted to gain a more complete assessment of effectiveness. If possible, at least three, and preferably more, such tests should be conducted. However, the assessor must recognize that once the first test is complete, the “word will spread” quickly and the protective force will be more alert. If possible, several locations should be tested in a short time interval; for example, tests conducted simultaneously at three different MAAs. Tests during high-traffic periods (for example, shift change) are desirable.

The locations selected for badge tests should be based on consideration of all pertinent factors, including:

- The potential impact of an unauthorized entry to the area
- Other complementary systems
- The number of layers in the system: LA, PA, MAA
- The number of personnel assigned to the area and the procedures for SPO rotation (personnel recognition)
- Throughput rates at portals.

Badge tests should be conducted as unobtrusively as possible in order to realistically simulate normal conditions. A crowd of observers will likely influence the actions of the SPO. If possible, the assessor should arrange to discreetly observe the test (for example, by CCTV at the CAS).

Responsibilities

Inspectors:	Select the type of fake badges needed and request the facility to provide them without alerting SPOs. Select the portal(s) that will be tested and the time(s) of the tests. Select and provide instructions to the adversaries.
Facility:	Provide fake badges as needed. Provide assistance in finding adversaries. Address safety concerns and ensure that protective force supervision is available to control response.

Internal Coordination

Test results are also of interest to the protective force topic team as they relate to training and duties. Tests should not be scheduled such that they would interfere with other tests involving the protective force.

Security Considerations

All normal security procedures should be followed. If an unauthorized person successfully gains access to a security area, measures should be taken to ensure that he/she is not permitted access to classified matter.

Logistical Requirements

- Fake badges may be needed from the badge office.
- A protective force supervisor should be available to control activities at each portal where a test is conducted.
- Observers, if any, should be kept from influencing the test results. Observation by CCTV at a remote location is desirable.

Safety

- Normal operating procedures should be followed.
- Protective force supervisors should ensure that the SPO's response can be controlled.
- A safety plan should be completed.

Personnel Assignments

Test Director:

Facility Trusted Agent:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator: